ANÁLISIS Y DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA FAVI DE LA UNIVERSIDAD TECNOLÓGICA DE PEREIRA

BRIAN DANIEL GARCÍA OSPINA

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

PEREIRA

2018

ANÁLISIS Y DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA FAVI DE LA UNIVERSIDAD TECNOLÓGICA DE PEREIRA

BRIAN DANIEL GARCÍA OSPINA

Práctica empresarial conducente a trabajo de grado para optar al título de Ingeniero de Sistemas y Computación

Director

JULIO CÉSAR LÓPEZ BETANCUR

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

PEREIRA

2018

AGRADECIMIENTOS

“Agradezco a mi familia por siempre brindarme su apoyo incondicional y ayuda incesante, a mi hermana Carolina por convertirse en una razón para ser una mejor persona cada día, a mi padre Jorge por su ayuda y enseñarme a valorar que cada gota de sudor cuenta, pero sobre todo a mi madre Luz Marina por su lealtad y sacrificio, por siempre estar ahí a pesar de las dificultades. Agradezco a la Cooperativa FAVI UTP y sus funcionarios por abrirme las puertas y acogerme como parte de ellos. Gracias al ingeniero Julio César López, por compartir conmigo su conocimiento, guía, seguimiento y constante retroalimentación. Gracias a ellos y a todos mis amigos, docentes y compañeros con los que tuve la oportunidad de compartir y quienes también me ayudaron a formarme como profesional y persona”

Brian Daniel Garcia Ospina

TABLA DE CONTENIDO

1. Introducción 8
2. Definición del problema 9
3. Justificación 10
4. Objetivos 12
   4.1 Objetivo General 12
   4.2 Objetivos Específicos 12
5. Metodología 13
6. Cronograma del proyecto 14
7. Marco Referencial 16
   7.1 Marco teorico 16
   7.1 Antecedentes 17
   7.2 Marco contextual 18
8. Procesos y procedimientos del Sistema de Gestión de Calidad actual 19
9. Estudio Norma ISO 27001 20
10. Encuesta diagnóstica de situación actual 21
11. Analisis del diagnostico 22
12. Alcance del Sistema de Gestión de Seguridad de la información 25
13. Politica del Sistema de Gestión de Seguridad de la información 28
14. Guía metodológica de análisis de riesgos de seguridad y privacidad de la información 62
15. Guía practica para la consolidación del componente de administración del riesgo 86
   15.1 Política de admnistración del riesgo 121
16. Declaración de aplicabilidad 122
17. Conclusiones 148
18. Bibliografia 149

LISTA DE FIGURAS

1. Mapa de procesos Cooperativa FAVI UTP 19
2. Estructura ISO 27001 20
3. Aspectos de la Gestión del riesgo 22
4. Evaluación de estado – Lista de chequeo diagnostica realizada..... 27
5. Conformidad de la lista de chequeo – Requisitos generales 29
6. Conformidad de la lista de chequeo – Requisitos generales 29
7. Conformidad por control – Requisitos generales 30
8. Conformidad por sección – Requisitos generales..... 30
9. Estado de conformidad por sección – Requisitos generales 31
10. Estado de conformidad por control – Requisitos generales..... 31
11. Plan de implementación – Requisitos generales 32
12. Plan de implementación – Requisitos generales 32
13. Conformidad de la lista de chequeo – Controles Anexo A..... 34
14. Conformidad de la lista de chequeo – Controles Anexo A..... 34
15. Conformidad por sección – Controles Anexo A 35
16. Conformidad por control – Controles Anexo A..... 35
17. Estado de conformidad por sección – Controles Anexo A..... 36
18. Estado de conformidad por control – Controles Anexo A 36
19. Plan de implementación – Controles Anexo A..... 37
20. Plan de implementación – Controles Anexo A..... 37
21. Cuerpo del correo institucional 60
22. Firma institucional..... 60
23. Riesgos de Seguridad y Privacidad de la Información..... 71
24. Mapa de Calor para la Representación de los niveles de Riesgo por Zonas.. 81
25. Matriz de Riesgos de Seguridad y Privacidad de la Información – Encabezado de la Matriz. 82
26. Matriz de Riesgos de Seguridad y Privacidad de la Información – Registro de Activos..... 82
27. Matriz de Riesgos de Seguridad y Privacidad de la Información – Calificación, Valoración y Análisis de Riesgo para los Activos de Información 83

28. Matriz de Riesgos de Seguridad y Privacidad de la Información – Valoración de Riesgos Inherentes y Riesgos Residuales para los Activos de Información 83
29. Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Encabezado de la Matriz Plan de Tratamiento 84
30. Tratamiento de Riesgos de Seguridad y Privacidad de la Información– Componentes de la Matriz Plan de Tratamiento 84
31. Tratamiento de Riesgos de Seguridad y Privacidad de la Información– Definiciones de Plan de Tratamiento 85
32. Mapa de procesos Cooperativa FAVI UTP 88
33. Matriz DOFA 89
34. Contexto estratégico 93
35. Descripción de riesgos 99
36. Clasificación de riesgos 101
37. Tipo de impacto 102
38. Matriz de Calificación y evaluación de los Riesgos por zonas de riesgo 103
39. Matriz opciones de manejo según la ubicación en las zonas de riesgo 105
40. Matriz de evaluación por zonas de riesgo (resultados probabilidad por impacto) 105
41. Matriz de probabilidad de impacto 106
42. Matriz de Calificación, Evaluación y Respuesta a los Riesgos 106
43. Probabilidad de impacto y zona de riesgo 107
44. Probabilidad de impacto y zona de riesgo 107
45. Controles de administración de riesgo 108
46. Ejemplo de redacción de un control 109
47. Preguntas de control 110
48. Análisis de controles de probabilidad 111
49. Análisis de controles de probabilidad 112
50. Análisis de controles de impacto 112
51. Análisis de controles de probabilidad 113
52. Rango de impacto 114
53. Resultado de la evaluación en el rango 0-50 114
54. Resultado de la evaluación en el rango 51-75 115

55. Resultado de la evaluación en el rango 76-100 115
56. Matriz de ubicación del riesgo 116
57. Preguntas de control 117
58. Nueva evaluación del riesgo 117
59. Tratamiento del riesgo 120

LISTA DE TABLAS

1. Factores de Riesgo asociados al SGSI 73
2. Criterios 76
3. Valoración de la Probabilidad de Ocurrencia 79
4. Valoración del Impacto 80
5. Dimensión de Riesgos 80
6. Zona de Riesgo 81

INTRODUCCIÓN

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo lo cual no solo repercute en costes económicos, sino que puede afectar considerablemente la imagen que tienen los asociados de su organización.

Es por esto por lo que se hace necesario brindar ayuda, soporte y control en los diferentes procesos tecnológicos dentro de la cooperativa, así como diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI) para ayudar a establecer políticas y procedimientos en relación con los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

DEFINICIÓN DEL PROBLEMA

La cooperativa FAVI UTP ofrece servicios con calidez, calidad y valor agregado, a través de un amplio portafolio de productos y servicios financieros flexibles, competitivos y personalizados, que contribuyan al mejoramiento de la calidad de vida de los asociados, colaboradores y comunidad, garantizando el desarrollo sostenible de cooperativa.

Por esto se hace necesario el diseño del planteamiento de un SGSI estructurado que permita dentro de la cooperativa garantizar la confidencialidad, integridad y disponibilidad de los datos de sus clientes, de su operación, de que los riesgos de la seguridad de la información sean reconocidos, asumidos, gestionados y minimizados de una forma ordenada, eficiente y adaptable a los cambios que se susciten en los riesgos, el entorno y las mismas tecnologías.

JUSTIFICACIÓN

Los sistemas de información poseen una estructura que permite transformar datos de entrada en datos de salida, los cuales pueden ser computarizados. De allí que estos sistemas de información sean contemplados como el sistema nervioso de una organización. El mal funcionamiento de uno de los sistemas puede causar fallas en todas la organizaciones y exposición a riesgos de pérdida o caída. Por ello, mantener un nivel alto de rendimiento en los sistemas de información, incluyendo el apropiado nivel de seguridad, puede tener un impacto directo en cómo las organizaciones responden ante crisis.

Las tres propiedades principales de un sistema de información para asegurar la seguridad de la información son confidencialidad, disponibilidad e integridad.

Confidencialidad es definida por la norma ISO 27001:2013 como “Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.” La mayoría de los sistemas son diseñados con una vista hacia la funcionalidad, la necesidad de confidencialidad es notada por los desarrolladores en las diferentes etapas de diseño de software. En vista de las tecnologías que actualmente se desarrollan y que son el auge actual como son plataformas web implementadas en la nube, asegurar la confidencialidad se convierte en un reto que incrementa cada vez más, sin dejar de lado la importancia de preservar la confidencialidad en todos los procesos realizados por la organización.

Problemas relacionados con la disponibilidad de la información, entendida como “Accesibilidad y usabilidad de acuerdo con la demanda” no son usualmente vistos como un problema dentro de las organizaciones, pues la falta de acceso a los datos se explica fácilmente con argumentos como caída de electricidad, virus o pérdida de acceso y algunas áreas de las organizaciones los ven como algo temporal. Sin embargo, la disponibilidad de la información es uno de los factores que pueden afectar la habilidad de las organizaciones para mantener la continuidad de sus operaciones. Estas pérdidas de continuidad pueden generar pérdidas financieras, pérdida de imagen e incluso la necesidad de parar las operaciones. Puede ser particularmente peligroso para compañías que debido a su estructura tecnológica requieren una operación continua.

La tercera propiedad principal de un sistema de seguridad de la información es la integridad, la cual es definida como “salvaguardar la aproximación y completitud de la información. Puede ser relacionada a la estructura y configuración de dispositivos de red y aplicaciones, pero, además los problemas de integridad se relacionan al como los trabajadores recolectan y procesan los datos. Fallas en la consecución de la integridad puede causar retrasos en la toma de decisiones hechas por la dirección y falta de acciones para minimizar los efectos de amenazas existentes.

Aparte de estas propiedades mencionadas, dentro de las organizaciones se debe dar gran importancia a otros atributos de la información, como, por ejemplo: la actualización, comparabilidad, procesabilidad, flexibilidad, eficiencia, costo, tiempo

de respuesta, estabilidad, detalle, direccionamiento, utilidad, prioridad, valor, facilidad de uso y seguridad.

El presente trabajo describe metodológicamente el diseño del Sistema de Gestión de Seguridad de la Información, para la Cooperativa FAVI UTP de la ciudad de Pereira, la cual en búsqueda de mitigar los riesgos respecto a sus activos de información busca garantizar estas propiedades esenciales mencionadas.

OBJETIVOS

GENERAL

Práctica empresarial: Diseño y análisis del sistema de gestión integrado bajo la norma ISO 27001:2013 para la cooperativa FAVI UTP, así como brindar ayuda, soporte y control en los diferentes procesos tecnológicos dentro de la cooperativa.

ESPECÍFICOS

- Hacer el diagnóstico y análisis inicial de buenas prácticas de seguridad de la información de la cooperativa FAVI UTP con respecto a la norma 27001.
- Analizar y construir artefactos necesarios para la planeación del SGSI.
- Diseñar el plan para la implementación del SGSI.

METODOLOGÍA

El proyecto de grado corresponde al análisis y diseño del sistema de gestión y seguridad de la información para la Cooperativa FAVI de la Universidad Tecnológica de Pereira, por medio de práctica empresarial conducente a trabajo de grado. Dicho diseño contempla el diagnóstico y análisis inicial de buenas prácticas de seguridad de la información basado en el estándar ISO/IEC 27001 de 2013, análisis y construcción de artefactos necesarios para la planeación y el plan para la implementación del SGSI.

La metodología se contempla a partir de entrevistas no estructuradas al coordinador de sistemas de la cooperativa FAVI UTP respecto a la ejecución de esta práctica empresarial, se trataron temas como el contexto de la organización, con que procesos cuenta la cooperativa, la complejidad de estos y los problemas actuales.

De allí se deduce el enfoque a utilizar el cual es la investigación descriptiva, donde se expondrá la situación actual del estado de la cooperativa respecto al sistema de gestión ISO 27001:2013.

La investigación descriptiva tiene como finalidad definir, clasificar, catalogar o caracterizar el objeto de estudio. Los métodos descriptivos pueden ser cualitativos o cuantitativos. La investigación descriptiva se aplicó definiendo la correlación de los numerales de las normas, clasificar y catalogar los datos definidos en las diferentes tablas y matrices expuestas en el trabajo. Los métodos cualitativos se basan en la utilización del lenguaje verbal y no recurren a la cuantificación. Los principales métodos de la investigación descriptiva son el observacional, el de encuestas y los estudios de caso único.

Debido a que la naturaleza del proyecto es el diseño de un sistema de gestión integrado, se ubica en la línea de investigación de gestión de la calidad: sublime de procesos para el diseño e implementación de sistemas integrados. El proyecto se llevará a cabo explorando las fuentes primarias de información como entrevistas y secundaria como archivos, tesis, análisis e información documentada que disponga la cooperativa FAVI UTP. La identificación y correlación de los requisitos aplicables al sistema de gestión ISO 27001 se realizará directamente mediante el uso de las normas NTC ISO disponibles por ICONTEC.

CRONOGRAMA DEL PROYECTO

		Duración en Meses																					
		2017																				2018	
Objetivo	Actividades	Oct		Nov				Dic				En				Feb				Mar			
Semana de inducción	Presentación del grupo de trabajo																						
	Visita instalaciones de la cooperativa sede Álamos																						
	Visita e instalación de puesto de trabajo en la sede de la Universidad Tecnológica de Pereira																						
	Reuniones con la Gerente de la cooperativa																						
	Reuniones con el Jefe de Sistemas de la cooperativa																						
Análisis y planeación SGSI	Lectura de los procesos y procedimientos del SGC Actual																						
	Realizar estudio de la norma ISO 27001																						
	Diseñar y Aplicar encuesta diagnóstica																						
	Análisis del diagnóstico																						
	Determinar el alcance del SGSI.																						
	Redactar la Política de SGSI.																						
	Identificar la metodología de evaluación de riesgos y determinar los criterios para la aceptabilidad de riesgos.																						
	Identificar activos, vulnerabilidades y amenazas.																						

	Evaluar la magnitud de los riesgos	
	Identificar y evaluar opciones para el tratamiento de riesgos.	
	Seleccionar controles para el tratamiento de riesgos.	
	Obtener la aprobación de la gerencia para la implementación del SGSI.	
	Redactar una declaración de aplicabilidad que detalle todos los controles aplicables y determine cuáles ya se han implementados y cuáles no son aplicables.	
	Preparación de la sustentación	
Actividades de Reacción	Brindar soporte técnico al manejo y desempeño del software y hardware	
Finalización de la Práctica Empresarial.	Sustentación de la Práctica Empresarial	

MARCO REFERENCIAL

MARCO TEÓRICO

Sistema de Gestión de Seguridad de la Información

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, así como los externos del entorno.

Sistema de Gestión de Calidad

El SGC (Sistema de Gestión de Calidad) es una herramienta que le permite a cualquier organización planear, ejecutar y controlar las actividades necesarias para el desarrollo de la misión, a través de la prestación de servicios con altos estándares de calidad, los cuales son medidos a través de los indicadores de satisfacción de los usuarios.

Norma NTC 9000:2005

La Norma ISO 9000 describe los fundamentos de los sistemas de gestión de la calidad y especifica la terminología de los sistemas de gestión de la calidad.

Norma NTC ISO 9001:2015

La norma ISO 9001 es una norma internacional de gestión de la calidad aplicable a cualquier tipo de organización de cualquier sector o actividad. Está basada en los ocho principios de gestión de calidad fundamentales para una buena gestión empresarial.

- Enfoque al cliente
- Liderazgo
- Compromiso de las personas
- Enfoque a procesos
- Mejora
- Toma de decisiones basada en la evidencia
- Gestión de las relaciones

Norma NTC ISO/IEC 27001:2013

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001

NTC ISO 31000:2011 GESTIÓN DEL RIESGO

La Gestión del Riesgo se hace necesaria para controlar y manejar las amenazas que se presentan a nivel organizacional y tecnológico, con los recursos disponibles, a fin de que no se materialicen estos riesgos y afecten los productos y/o servicios que ofrece la empresa.

Todas las actividades de una organización implican riesgo. Las organizaciones gestionan el riesgo mediante su identificación y análisis, luego evaluando si el riesgo se debería modificar por medio del tratamiento del riesgo con el fin de satisfacer los criterios del riesgo. A través de este proceso, las organizaciones se comunican y consultan con las partes involucradas, monitorean y revisan el riesgo y los controles que lo están modificando con el fin de garantizar que no se requiere tratamiento adicional del riesgo. Esta norma describe este proceso sistemático y lógico en detalle.

ANTECEDENTES

A fin de lograr realizar un análisis y diseño del Sistema de Gestión de Seguridad de la información, se consultó:

Modelo de seguridad y privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC el cual brinda los lineamientos apropiados para que las entidades públicas realicen buenas prácticas de seguridad de acuerdo con la norma 27001 del 2013 para su gestión de la información y con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Trabajo de grado “Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda” elaborado por los ingenieros egresados de la Universidad Tecnológica de Pereira Aguirre Cardona Juan David y Aristizábal Betancourt Catalina en la cual diseñan un SGSI que permita a la entidad tratar los activos de información en busca de tener un nivel de seguridad óptimo.

Sistemas de gestión implementados en organizaciones y entidades públicas del estado colombiano y las cuales hacen uso adecuado de las normas.

El producto final es entregado a la Cooperativa FAVI UTP y es de su uso exclusivo, por lo que en el siguiente se muestra cómo se realizó el análisis y diseño del Sistema de Gestión de Seguridad de la Información sin publicar y sin afectar la condición de confidencialidad de los datos que son de su propiedad.

MARCO CONTEXTUAL

La Cooperativa FAVI UTP esta especializada en ahorro y crédito, fundada en 1976 y ubicada con una sede central en la Carrera 27 No. 10-02 Barrio Álamos (Universidad Tecnológica de Pereira). Y otra sede en la Calle 13 No. 22-59 Local 1 Edificio Álamos reservado de la ciudad de Pereira, Risaralda.

La Cooperativa FAVI UTP contribuye a mejorar la calidad de vida de sus asociados con responsabilidad social; a través de una cultura de servicio, innovación y competitividad. Espera consolidarse en el año 2025 como una organización competitiva del sector solidario, con crecimiento sostenible y con productos y servicios innovadores; logrando un alto empoderamiento de sus asociados. Su política de calidad es facilitar y brindar servicios y productos financieros bajo los principios y valores cooperativos a través de una cultura de servicio y procesos de mejoramiento continuo, que conduzcan a la competitividad.

PROCESOS Y PROCEDIMIENTOS DEL SGC ACTUAL

Se realizó lectura de los procesos y procedimientos del Sistema de Gestión de Calidad que están presentes en la Cooperativa, enfatizando en el Manual de Procesos y Procedimientos, donde se describen las actividades compartidas y los responsables de los procesos que se realizan para la funcionalidad de la Cooperativa, integrando la documentación total implementada por la actual Administración, generando el compromiso de la dirección de la ejecución y la revisión permanente para la debida actualización. El mapa de procesos incluye las siguientes perspectivas:

- **De gestión o estratégicos.** Direccionan la entidad en el entorno dinámico, para prepararla a enfrentar oportunidades y desafíos que la posicionan ante la sociedad y sus asociados.
- **Misionales.** Son los procesos que desarrollan la misión, la razón de ser, la transformación de productos o servicios.
- **De apoyo o logísticos.** En donde se encuentran labores de administración de talento humano, compras – sistemas.
- **De Gestión de Control.** Facilitan el seguimiento al cumplimiento de las actividades tales como, los procesos, Documental. Interno y fiscal, Mejora Continua

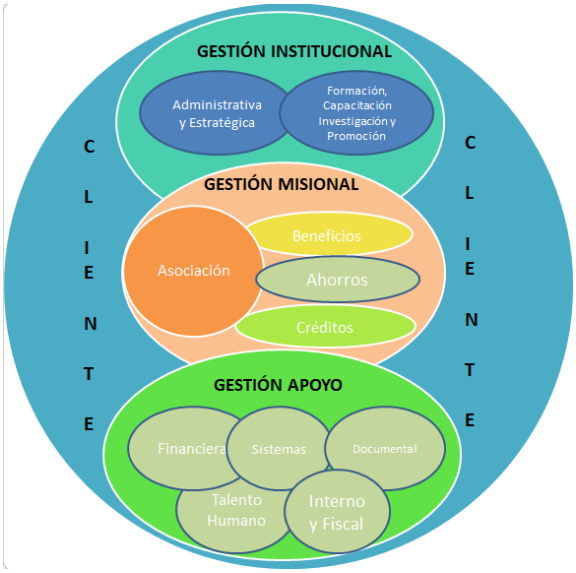


Figura # 1 Mapa de procesos Cooperativa FAVI UTP

Mapa de Procesos. Distribución de los procesos de acuerdo con los distintos procedimientos que componen los mapas específicos y con base en las líneas definidas como Gestión Institucional o Estratégica, Gestión misional o Central, Gestión Operativa o de Apoyo y la Gestión de Control, esta última transversal a todos los procesos.

Procesos: Permite contar con formas organizativas ágiles, dividir el trabajo por responsabilidades y compromisos, trabajar en equipo y con equipos de

trabajo definidos, facilitar la revisión y actualización de los procedimientos determinados por cada proceso definido, normalizar las actividades, formular los indicadores, hacer seguimiento y establecer las acciones o planes de mejora.

Procedimientos: Guías de acción detalladas de forma que pueda ejecutarse las actividades relacionadas conforme a una secuencia cronológica de las actividades requeridas, concatenadas entre sí, orientando la realización de estas y las tareas específicas.

NORMA ISO 27001

¿Cómo funciona la ISO 27001?

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están y luego tratarlos sistemáticamente.

Figura # 2 Estructura ISO 27001

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo: software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero lo utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar

todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

¿Por qué ISO 27001 es importante para una empresa?

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

Cumplir con los requerimientos legales – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

Obtener una ventaja comercial – si la empresa obtiene la certificación y sus competidores no, es posible que obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

Menores costos – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

¿Dónde interviene la gestión de seguridad de la información en una empresa?

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información.

Figura # 3 Aspectos de la Gestión del riesgo

¿Cómo es realmente ISO 27001?

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – Términos y definiciones – de nuevo, hace referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PHVA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PHVA y define las responsabilidades de la dirección, el establecimiento de

roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PHVA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PHVA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PHVA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PHVA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PHVA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Anexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

¿Cómo implementar ISO 27001?

Para implementar la norma ISO 27001 en una empresa, se deben seguir estos 16 pasos:

1) Obtener el apoyo de la dirección

2) Utilizar una metodología para gestión de proyectos

3) Definir el alcance del SGSI

4) Redactar una política de alto nivel sobre seguridad de la información

5) Definir la metodología de evaluación de riesgos

6) Realizar la evaluación y el tratamiento de riesgos

7) Redactar la Declaración de aplicabilidad

8) Redactar el Plan de tratamiento de riesgos

9) Definir la forma de medir la efectividad de sus controles y de su SGSI

10) Implementar todos los controles y procedimientos necesarios

11) Implementar programas de capacitación y concienciación

12) Realizar todas las operaciones diarias establecidas en la documentación de su SGSI

13) Monitorear y medir su SGSI

14) Realizar la auditoría interna

15) Realizar la revisión por parte de la dirección

16) Implementar medidas correctivas

Documentación obligatoria

ISO 27001 requiere que se confeccione la siguiente documentación:

- Alcance del SGSI (punto 4.3)
- Objetivos y política de seguridad de la información (puntos 5.2 y 6.2)
- Metodología de evaluación y tratamiento de riesgos (punto 6.1.2)
- Declaración de aplicabilidad (punto 6.1.3 d)
- Plan de tratamiento de riesgos (puntos 6.1.3 e y 6.2)
- Informe de evaluación de riesgos (punto 8.2)
- Definición de roles y responsabilidades de seguridad (puntos A.7.1.2 y A.13.2.4)
- Inventario de activos (punto A.8.1.1)
- Uso aceptable de los activos (punto A.8.1.3)
- Política de control de acceso (punto A.9.1.1)
- Procedimientos operativos para gestión de TI (punto A.12.1.1)
- Principios de ingeniería para sistema seguro (punto A.14.2.5)
- Política de seguridad para proveedores (punto A.15.1.1)
- Procedimiento para gestión de incidentes (punto A.16.1.5)
- Procedimientos para continuidad del negocio (punto A.17.1.2)
- Requisitos legales, normativos y contractuales (punto A.18.1.1)

Y estos son los registros obligatorios:

- Registros de capacitación, habilidades, experiencia y calificaciones (punto 7.2)
- Monitoreo y resultados de medición (punto 9.1)
- Programa de auditoría interna (punto 9.2)
- Resultados de auditorías internas (punto 9.2)
- Resultados de la revisión por parte de la dirección (punto 9.3)
- Resultados de medidas correctivas (punto 10.1)
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (puntos A.12.4.1 y A.12.4.3)

Por supuesto que una empresa puede decidir confeccionar otros documentos de seguridad adicionales si lo considera necesario.

Revisiones 2005 y 2013 de ISO 27001

La norma ISO 27001 fue publicada por primera vez en 2005 y luego fue revisada en 2013; por lo tanto, la versión válida actual es la ISO/IEC 27001:2013.

Los cambios más importantes de la revisión 2013 están relacionados con la estructura de la parte principal de la norma, las partes interesadas, los objetivos, el monitoreo y la medición; asimismo, el Anexo A ha disminuido la cantidad de controles (de 133 a 114) y ha incrementado la cantidad de secciones (de 11 a 14). En la revisión 2013 se eliminaron algunos requerimientos como las medidas preventivas y la necesidad de documentar determinados procedimientos.

Sin embargo, todos estos cambios en realidad no modificaron mucho la norma en su conjunto, su filosofía principal sigue centrándose en la evaluación y tratamiento de riesgos y se mantienen las mismas fases del ciclo de Planificación, Implementación, Revisión y Mantenimiento (PHVA, por sus siglas en inglés). Esta nueva revisión de la norma es más fácil de leer y comprender y es mucho más sencilla de integrar con otras normas de gestión como ISO 9001, ISO 22301, etc.

Las empresas que han sido certificadas en ISO/IEC 27001:2005 deben hacer la transición a la nueva revisión 2013 hasta septiembre de 2015 si quieren mantener la validez de su certificación.

Otras normas relacionadas con seguridad de la información

ISO/IEC 27002 proporciona directrices para la implementación de los controles indicados en ISO 27001. ISO 27001 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO 27002 puede ser bastante útil ya que proporciona más información sobre cómo implementar esos controles. A la ISO 27002 anteriormente se la conocía como ISO/IEC 17799 y surgió de la norma británica BS 7799-1.

ISO/IEC 27004 proporciona directrices para la medición de la seguridad de la información; se acopla bien con ISO 27001 ya que explica cómo determinar si el SGSI ha alcanzado los objetivos.

ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de información. Es un muy buen complemento para ISO 27001 ya que brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación. ISO 27005 ha surgido de la norma británica BS 7799-3.

ISO 22301 define los requerimientos para los sistemas de gestión de continuidad del negocio, se adapta muy bien con ISO 27001 porque el punto A.17 de esta última requiere la implementación de la continuidad del negocio, aunque no proporciona demasiada información.

ISO 9001 define los requerimientos para los sistemas de gestión de calidad. Aunque a primera vista la gestión de calidad y la gestión de seguridad de la información no tienen mucho en común, lo cierto es que aproximadamente el 25% de los requisitos de ISO 27001 y de ISO 9001 son los mismos: control de documentos, auditoría interna, revisión por parte de la dirección, medidas

correctivas, definición de objetivos y gestión de competencias. Esto quiere decir que si una empresa ha implementado ISO 9001 le resultará mucho más sencillo implementar ISO 27001.

ENCUESTA DIAGNÓSTICA DE SITUACIÓN ACTUAL

Se empleó una herramienta de diagnóstico o lista de chequeo la cual puede ser utilizada para desarrollar la primera etapa del ciclo de mejoramiento continuo, es decir el PLANEAR. No es lo mismo que llevar a cabo una auditoría, ya que el personal de la cooperativa participa en el mismo diagnóstico, por lo que no se cumple principios de la auditoría como objetividad, imparcialidad, autonomía e independencia.

Uno de los propósito del diagnóstico es establecer un plan de implementación para organizaciones que desean implementar la norma en la versión 2013 así como identificar puntos débiles y opciones de mejora a revisar.

En su primera parte, se cuenta con conformidades que hacen referencia a los capítulos de la norma ISO 27001: 2013 desde el capítulo 4 al 10, en donde se presenta una lista de chequeo de acuerdo a los requisitos que deben evaluarse.

La segunda parte cuenta con controles del anexo A de la norma ISO 27001:2013, en donde se presenta la lista de chequeo de acuerdo a los controles que se deben implementar en el Sistema de Gestión de Seguridad de la Información.

Estas partes al final obtienen un RESUMEN CONSOLIDADO en donde se encuentran los gráficos y la información del diagnóstico consolidada.

COOPERATIVA FAVI UTP	ISO 27001: 2013 Evaluación de estado	ISO 27001:2013
ENTIDAD EVALUADA	Cooperativa FAVI UTP	
FECHAS DE EVALUACIÓN	10/11/2017 VERSION 1.0	
CONTACTO	Julio Cesar Lopez Betancur	
ELABORADO POR	Brian Daniel Garcia Ospina	

Figura # 4 Evaluación de estado – Lista de chequeo diagnostica realizada a la Cooperativa FAVI UTP

ANALISIS DEL DIAGNOSTICO

La lista de chequeo diagnostica se aplicó a la Cooperativa FAVI UTP con el fin de obtener una mirada al estado en el cual se encuentra antes de la implementación del Sistema de Gestión de Seguridad de la Información y ver en qué casos se da cumplimiento a los requisitos y controles establecidos por la norma ISO 27001:2013.

Una vez realizada la evaluación de nivel de cumplimiento se procede a establecer el plan de acción a seguir para la implementación del Sistema de Gestión de Seguridad de la Información y el cual comprende:

- Secciones de la norma ISO 27001:2013
- Que hace falta para la implementación del Sistema de Gestión de seguridad de la Información
- Las actividades por realizar
- La descripción de las metas y resultados esperados
- Fecha de culminación de las actividades
- Procesos involucrados
- Responsables de estos procesos
- Presupuesto involucrado por parte de la cooperativa

Requisitos generales

En la conformidad de la lista de chequeo, se estableció una valoración de los resultados obtenidos reflejados en el porcentaje de nivel de cumplimiento tanto de los requisitos generales como los controles de la norma a fin de identificar el estado actual de la cooperativa. En base al ítem de la norma ISO y su respectivo control, se define en base a las entrevistas a funcionarios y revisión documental:

- Que se tiene: Se define con que cuenta la cooperativa que sea importante para la seguridad de la información.

- Que hace falta: De acuerdo con la norma se verifica que hace falta para que se cumpla con un nivel de cumplimiento superior.

- Recomendaciones: Se define que esfuerzos debe llevar a cabo la cooperativa a fin de alcanzar el nivel de cumplimiento.

De allí se establece un nivel de cumplimiento de conformidad por control y por sección en los cuales se da un resumen general promedio de los resultados obtenidos en la lista de chequeo y se procede posteriormente a realizar unas graficas evaluativas del estado de conformidad de la cooperativa respecto a los controles y secciones.

Referencia			
Lista de verificación	ISO	Control	Que se tiene
	4	CONTEXTO DE LA ORGANIZACIÓN	
	4,1	CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	
	4.1.1	La organización debe determinar: Las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.	
	4,2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	
	4.2.1	La organización debe determinar: Las partes interesadas que son pertinentes al sistema de gestión de seguridad de la informacion;	

Figura # 5 Conformidad de la lista de chequeo – Requisitos generales

	resultados	
Que hace falta	Recomendaciones	NIVEL DE CUMPLIMIENTO
		100%
		100%

Figura # 6 Conformidad de la lista de chequeo – Requisitos generales

Estándar	Sección	estatus
4,1	CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	
4,2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	
4,3	DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
4,4	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
5,1	LIDERAZGO Y COMPROMISO	
5,2	POLÍTICA	
5,3	ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	
6,1	ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	
6,2	OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS.	
7,1	RECURSOS	
7,2	COMPETENCIA	
7,3	TOMA DE CONCIENCIA	
7,4	COMUNICACIÓN	
7,5	INFORMACIÓN DOCUMENTADA	
8,1	PLANIFICACIÓN Y CONTROL OPERACIONAL	
8,2	VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	
8,3	TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	
9,1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	
9,2	AUDITORIA INTERNA	
9,3	REVISIÓN POR LA DIRECCIÓN	
10,1	NO CONFORMIDAD Y ACCIÓN CORRECTIVA	
10,2	MEJORA CONTINUA	

Figura # 7 Conformidad por control – Requisitos generales

Estándar	Sección	estatus
4	CONTEXTO DE LA ORGANIZACIÓN	
5	LIDERAZGO	
6	PLANIFICACIÓN	
7	SOPORTE	
8	OPERACIÓN	
9	EVALUACIÓN DEL DESEMPEÑO	
10	MEJORA	

El cumplimiento global	

Figura # 8 Conformidad por sección – Requisitos generales

Figura # 9 Estado de conformidad por sección – Requisitos generales

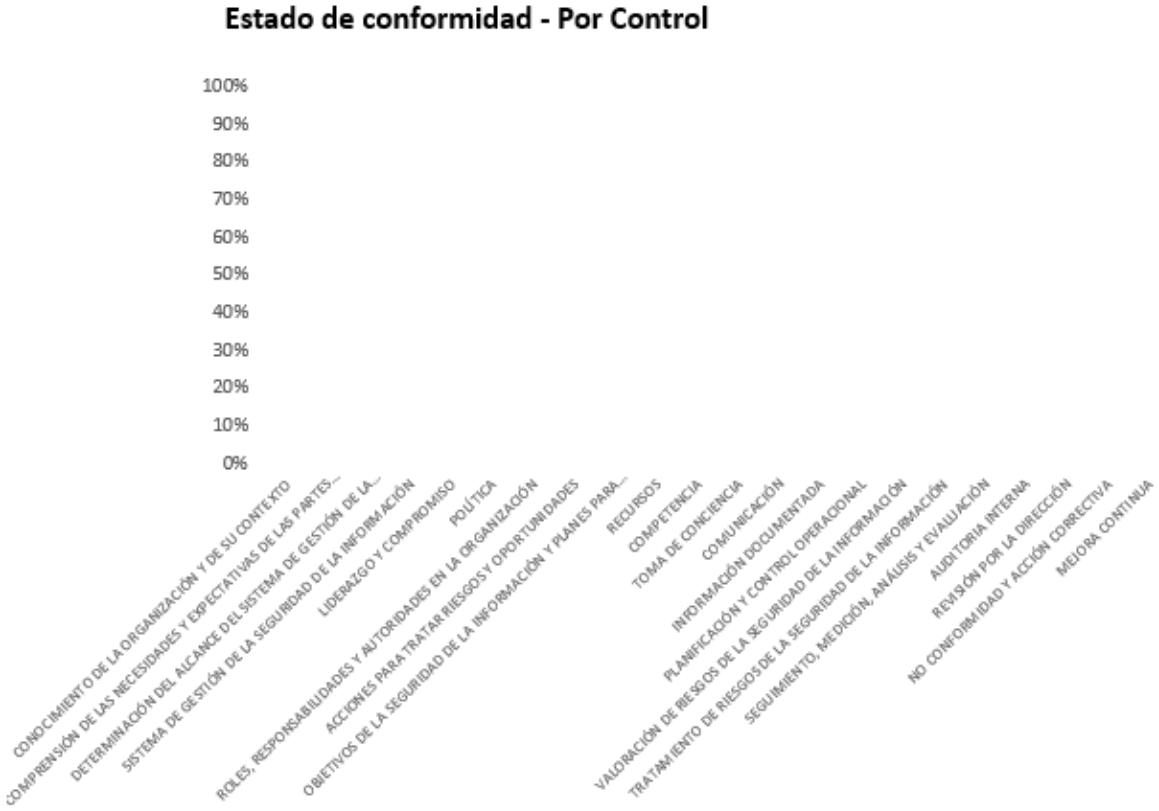


Figura # 10 Estado de conformidad por control – Requisitos generales

Seccion de la norma ISO 27001:2013	PLAN DE IMPLEMENTACIÓN SISTEMA DE GESTIO		
	QUE NOS FALTA	ACTIVIDADES	Descripción Metas Resultados esperados
4.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO			
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS			

Figura # 11 Plan de implementación – Requisitos generales

ÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
Fecha culminación	Procesos involucrados	Responsables	Presupuesto

Figura # 12 Plan de implementación – Requisitos generales

Controles anexo A

En los controles la conformidad de la lista de chequeo difiere en que se establece un área de evaluación de cumplimiento, una prueba y una justificación, se definen entonces:

- Sección: Ítem de la norma ISO 27001:2013.

- Control: Lo que se debe llevar a cabo para dar el correspondiente cumplimiento.

- Puntos de evaluación inicial: Preguntas realizadas al coordinador de sistemas y funcionarios a fin de verificar el estado actual y cumplimiento.

- Prueba: Pasos que se deben seguir para evidenciar el cumplimiento.

- Que se tiene: Se define con que cuenta la cooperativa que sea importante para la seguridad de la información.

- Que hace falta: De acuerdo con la norma se verifica que hace falta para que se cumpla con un nivel de cumplimiento superior.

- Justificación: Se define si el control es incluido como parte integral de los requisitos del estándar para el SGSI de la cooperativa.

Referencia		Área de Evaluación de Cumplimiento		
Lista de verificación	ISO	Sección	Control	Puntos evaluación inicial
	A.5	Políticas de Seguridad		
	A.5.1	Orientación de la Dirección para la Gestión de la Seguridad de la Información		
	A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	1. Existen políticas de seguridad ? 2. ¿todas las políticas son aprobadas por la administración? 3. ¿Las políticas se comunican adecuadamente a los empleados?
	A.5.1.2	Revisión de las políticas de seguridad de la información	Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	1. ¿ las políticas de seguridad son sujetas a revisión? 2. ¿ los exámenes son realizados a intervalos regulares? 3. ¿los exámenes son realizados cuando cambian las circunstancias?

Figura # 13 Conformidad de la lista de chequeo – Controles Anexo A

			resultados	
Prueba	Que se tiene	Que hace falta	Justificación	NIVEL DE CUMPLIMIENTO
Solicite la política de seguridad de la información de la cooperativa y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la cooperativa c) Si fue debidamente aprobada y socializada al interior de la cooperativa por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas.			Se incluye como parte integral de los requisitos del estándar para el SGSI de la cooperativa.	100%
Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual.			Se incluye como parte integral de los requisitos del estándar para el SGSI de la cooperativa.	100%

Figura # 14 Conformidad de la lista de chequeo – Controles Anexo A

Estándar	Sección	estatus
A.5	Políticas de Seguridad	
A.6	Organización de la seguridad de la información	
A.7	la seguridad de los recursos humanos	
A.8	Gestión de activos	
A.9	Control de acceso	
A.10	Criptografía	
A.11	La seguridad física y ambiental	
A.12	seguridad de las operaciones	
A.13	seguridad de las comunicaciones	
A.14	Sistema de adquisición, desarrollo y mantenimiento	
A.15	relaciones con los proveedores	
A.16	gestión de incidentes de seguridad de información	
A.17	los aspectos de seguridad de información de gestión de la continuidad del negocio	
A.18	Conformidad	

El cumplimiento global	

Figura # 15 Conformidad por sección – Controles Anexo A

Estándar	Sección	estatus
A.5.1	Dirección de gestión de seguridad de la información	
A.6.1	Organización interna	
A.6.2	Los dispositivos móviles y el teletrabajo	
A.7.1	Antes de empleo	
A.7.2	durante el empleo	
A.7.3	Terminación y cambio de empleo	
A.8.1	Responibility para los activos	
A.8.2	clasificación de la información	
A.8.3	La gestión de medios	
A.9.1	Los requisitos de negocio para el control de acceso	
A.9.2	gestión de acceso de los usuarios	
A.9.3	responsabilidades de los usuarios	
A.9.4	Sistema de control de acceso a las aplicaciones y	
A.10.1	controles Crypographic	
A.11.1	Las áreas seguras	
A.11.2	Equipo	
A.12.1	los procedimientos y las responsabilidades operativas	
A.12.2	Protección contra el malware	
A.12.3	Apoyo	
A.12.4	Registro y supervisión	
A.12.5	El control de software operacional	
A.12.6	La gestión técnica de la vulnerabilidad	
A.12.7	consideraciones de auditoría de sistemas de información	
A.13.1	gestión de seguridad de la red	
A.13.2	La transferencia de información	
A.14.1	Los requisitos de seguridad de los sistemas de información	
A.14.2	Seguridad en los procesos de desarrollo y soporte	
A.14.3	Datos de prueba	
A.15.1	seguridad de la información en relación con los proveedores	
A.15.2	la gestión de la prestación de servicios de proveedores	
A.16.1	Gestión de incidentes y mejoras infosec	
A.17.1	la continuidad seguridad de la información	
A.17.2	redundancias	
A.18.1	El cumplimiento de los requisitos legales y contractuales	
A.18.2	opiniones seguridad de la información	

Figura # 16 Conformidad por control – Controles Anexo A

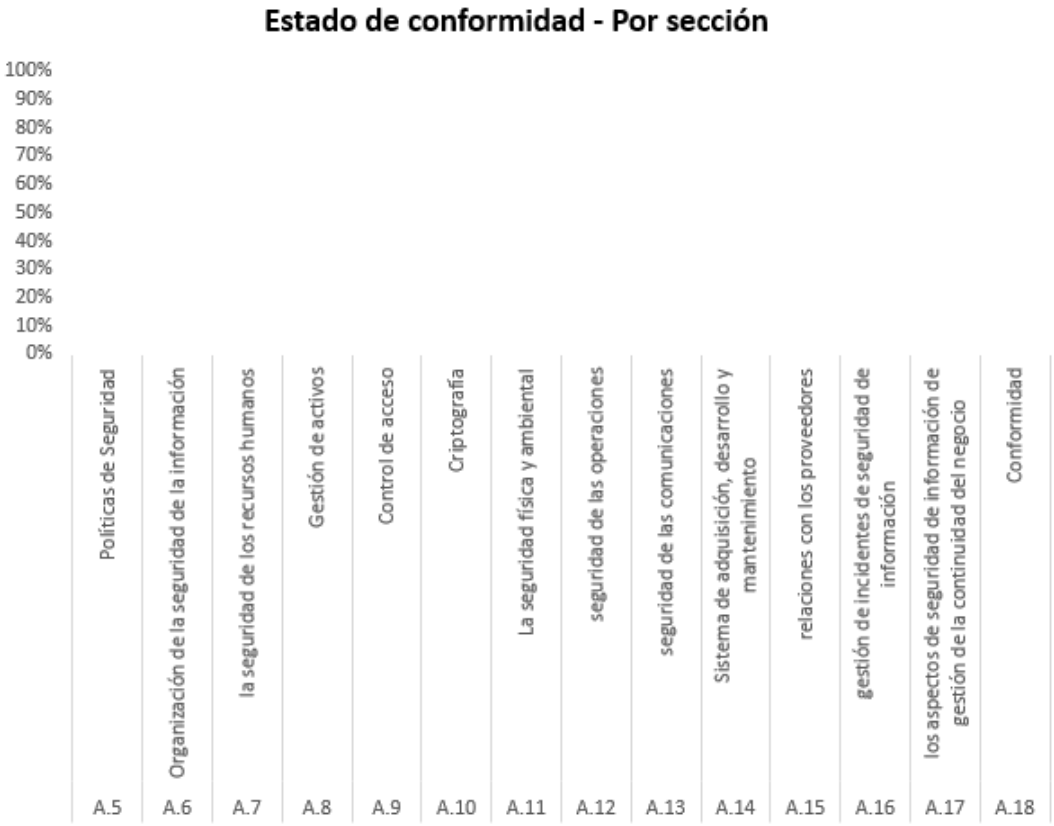


Figura # 17 Estado de conformidad por sección – Controles Anexo A

Figura # 18 Estado de conformidad por control – Controles Anexo A

Seccion de la norma ISO 27001:2013	PLAN DE IMPLEMENTACIÓN SISTEMA DE GESTION DE LA S		
	QUE NOS FALTA	ACTIVIDADES	Descripción Metas Resultados esperados
A.5.1 Orientación de la Dirección para la Gestión de la Seguridad de la Información			
A.6.1			

Figura # 19 Plan de implementación – Controles Anexo A

SEGURIDAD DE LA INFORMACIÓN		Responsables	Presupuesto
Fecha culminación	Procesos involucrados		

Figura # 20 Plan de implementación – Controles Anexo A

ALCANCE

La cooperativa FAVI UTP con el sistema de gestión de seguridad de la información busca establecer políticas, guías y controles para conservar la integridad, disponibilidad y confidencialidad de la información.

1. Objetivo

Establecer el alcance, así como los roles y responsabilidades en el SGSI a implementar en la cooperativa FAVI UTP

2. Alcance

El Sistema de Gestión de Seguridad de la información debe ser aplicado en todos los activos de la cooperativa FAVI UTP, en sus procesos y en sus plataformas tecnológicas.

a) Activos

Dentro del alcance del SGSI están:

(i) Los activos de información identificados en los procesos de la cooperativa.

(ii) Los contenedores donde se alojan dichos activos de información.

(iii) El área de investigación comprende el interior de la cooperativa FAVI UTP.

(iv) La sede principal de la cooperativa FAVI UTP ubicada en la Carrera 27 No. 10-02 Barrio Álamos. Universidad Tecnológica de Pereira. Y la sede reservada ubicada en la Calle 13 No. 22-59 Local 1 Edificio Álamos.

(v) Sus colaboradores, proveedores, contratistas y asociados.

b) Plataformas tecnológicas

Las plataformas tecnológicas que hacen parte del alcance del SGSI son:

(i) Sitio web de la cooperativa FAVI UTPwww.faviutp.com

(ii) Plataforma VISIONAMOS

c) Procesos

Hacen parte del alcance del SGSI todos los procesos descritos en el mapa de procesos de la cooperativa FAVI UTP, que están clasificados dentro de los marcos de gestión institucional, misional y de apoyo.

3. Roles y responsabilidades del SGSI

Todos los funcionarios de la cooperativa FAVI UTP son responsables de la seguridad de la información. Adicionalmente existen los siguientes roles y responsabilidades específicas dentro del SGSI.

a) Consejo de administración de la cooperativa FAVI UTP

El consejo de administración de la cooperativa FAVI UTP, es el encargado de la implementación de las líneas estratégicas: desarrollo organizacional, innovación e investigación, así como está encargado de las siguientes responsabilidades:

(i) Definir la estrategia, el gobierno y la dirección de la gestión de la seguridad de la información.

(ii) Aprobar la política de seguridad y privacidad de la información.

(iii) Promover la gestión de la seguridad de la información mediante el compromiso de la dirección y la asignación de los recursos adecuados.

(iv) Estudiar y aprobar las iniciativas de seguridad de la información que le sean propuestas.

b) Responsable del funcionamiento del SGSI

El responsable del funcionamiento del SGSI en la cooperativa FAVI UTP es el Coordinador de Sistemas. Sus principales responsabilidades son:

(i) Asegurar la disponibilidad de los recursos necesarios para la definición, la implementación y el mantenimiento del SGSI.

(ii) Revisar periódicamente los documentos y controles del SGSI para asegurar que el SGSI logre los resultados previstos.

(iii) Analizar los incidentes de seguridad que le sean escalados y ponerse en contacto con las autoridades correspondientes.

(iv) Definir lineamientos que den guía al oficial de seguridad de la información.

(v) Coordinar con los propietarios de los activos de información y los dueños de procesos las acciones para el cumplimiento del SGSI.

(vi) Hacer el seguimiento a la implementación y el cumplimiento de los controles de seguridad en la cooperativa FAVI UTP
(vii) Apoyar a los funcionarios y contratistas para que cumplan con las responsabilidades de su rol frente al SGSI.
(viii) Liderar el proceso de gestión de incidentes de seguridad de la información en la cooperativa FAVI UTP

c) Propietario de los activos de información

Es el funcionario, contratista o área de la cooperativa FAVI UTP al cual se le ha asignado la responsabilidad formal sobre un activo de información. Sus principales responsabilidades son:

(i) Cumplir con la política de seguridad de la información aprobada por el consejo de administración.
(ii) Identificar, establecer el alcance y el valor o criticidad de los activos de información de los cuales es propietario.
(iii) Clasificar los activos de información siguiendo la metodología de identificación y clasificación de activos aprobada por el responsable del funcionamiento del SGSI.
(iv) Identificar, definir y evaluar los riesgos a los que pudieran estar expuestos los activos de información de los cuales es propietario.
(v) Definir los requerimientos de seguridad de los activos de información en relación con su confidencialidad, integridad y disponibilidad.
(vi) Informar los requerimientos y controles requeridos por los activos de información a los custodios y usuarios de los activos de información.
(vii) Efectuar una verificación periódica de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad.

(d) Custodio de los activos de información

Es el funcionario, contratista o área de la cooperativa FAVI UTP responsable de administrar y hacer efectivos los controles que el propietario del activo de información haya definido. Sus principales responsabilidades son:

(i) Implementar y mantener los controles requeridos en los contenedores donde estén almacenados los activos de información que se encuentren a su cargo.
(ii) Administrar los recursos donde residen los activos de información dando los permisos definidos por el propietario del activo a los usuarios interesados.

(iii) Proteger los activos de información presentes en los contenedores a su cargo en la situación que corresponda: almacenamiento, transporte y procesamiento.

(e) Dueño de procesos

Es el funcionario, contratista o área de la cooperativa FAVI UTP al cual se le ha asignado la responsabilidad formal sobre un proceso de la cooperativa. Sus principales responsabilidades son:

(i) Apoyar la identificación de los activos de información que intervienen en el proceso correspondiente.
(ii) Validar los activos de información identificados junto con las características básicas de cada uno de ellos.
(iii) Apoyar y validar la identificación y designación de los propietarios de los activos de información de su proceso.

(f) Usuario de la información

Es el funcionario o contratista de la cooperativa FAVI UTP que utiliza la información para desempeñar sus funciones. Sus principales responsabilidades son:

(i) Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones dentro y fuera de la cooperativa FAVI UTP.
(ii) Conocer la clasificación de los activos de información que maneja.
(iii) Preservar la seguridad de la información utilizada en el desempeño de sus funciones y obligaciones.
(iv) No divulgar la información clasificada sin autorización del propietario del activo de información.
(v) Procurar el buen manejo de todos los activos, buscando protegerlos en relación con los principios de seguridad.

POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. Objetivo

Presentar en forma clara y coherente las Políticas de tercer nivel del sistema de gestión de seguridad de la Información que deben conocer y cumplir todos los colaboradores, contratistas, proveedores de servicios y partes interesadas.

2. Alcance

Inicia con la creación de las políticas de cumplimiento de la norma NTC IEC 27001:2013 vigente, continúa con la divulgación del presente documento a todos los colaboradores, contratistas, proveedores y partes interesadas que laboren o tengan relación con la cooperativa FAVI UTP y termina con la aplicación, cumplimiento, adecuado uso de los niveles de seguridad de la Información.

3. Contexto

El presente documento tiene como objetivo brindar las herramientas apropiadas para dar cumplimiento a las políticas establecidas por la cooperativa FAVI UTP que busca garantizar la integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la cooperativa, brindando así una guía clara para todos sus colaboradores, proveedores y contratistas en cabeza del Gerente de la cooperativa.

Dentro del presente documento, se describen las políticas específicas de seguridad de la Información que se deberán conocer y cumplir por todos los colaboradores y terceras partes de la cooperativa FAVI UTP que accedan a los activos información.

4. Ámbito de aplicación

El presente documento, aplica a la operación de la cooperativa y los activos de información involucrados, dentro de los procesos y procedimientos.

5. Términos y definiciones

Para una mejor comprensión del presente documento se toman como referencia los presentes términos y definiciones establecidos en la Norma ISO 27000:

A

- **Aceptación del riesgo**: (Inglés: Risk acceptance). Decisión informada de asumir un riesgo concreto.

- **Activo:** (Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Alcance del sistema de seguridad**: (Inglés: Scope). Ámbito de la organización que queda sometido al SSI.

- **Amenaza**: (Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis de riesgos**: (Inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Análisis de riesgos cualitativo**: (Inglés: Qualitative risk analysis). Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

- **Análisis de riesgos cuantitativo**: (Inglés: Quantitative risk analysis). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

- **Autenticación:** (inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.

- **Autenticidad**: (Inglés: Authenticity). Propiedad de que una entidad es lo que afirma ser.

C

- **CID:** (Inglés: CIA). Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.

- **Confidencialidad:** (Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Control correctivo:** (Inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

- **Control detectivo**: (Inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

- **Control disuasivo**: (Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

D

- **Declaración de aplicabilidad**: (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

- **Desastre**: (Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

- **Directiva o directriz**: (Inglés: Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

- **Disponibilidad:** (Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

E

- **Estimación de riesgos**: (Inglés: Risk evaluation). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

- **Evaluación de riesgos**: (Inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.

G

- **Gestión de claves**: (Inglés: Key management). Controles referidos a la gestión de claves criptográficas.

- **Gestión de incidentes de seguridad de la información**: (Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Gestión de riesgos**: (Inglés: Risk management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

I

- **Identificación de riesgos**: (Inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.

- **IEC:** International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

- **Impacto:** (Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

- **Incidente de seguridad de la información**: (Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad**: (Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.

- **Inventario de activos**: (Inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **ISO/IEC 27001**: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

N

- **No conformidad**: (Inglés: Nonconformity). Incumplimiento de un requisito.

- **No repudio**: Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

O

- Objetivo de seguridad de la información: (Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

P

- **Parte interesada:** (Inglés: Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de continuidad del negocio**: (Inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos**: (Inglés: Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

R

- **Recursos de tratamiento de** información: (Inglés: Information processing facilities). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

S

- **Seguridad de la información**: (Inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Selección de controles:** (Inglés: Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

T

- **Trazabilidad**: (Inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

V

- **Vulnerabilidad:** (Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. Rol del coordinador de sistemas y/o practicante de sistemas respecto a la seguridad de la información

Será el responsable por la implementación, operación, mantenimiento y mejoramiento del sistema de gestión de seguridad en la Información en la cooperativa FAVI UTP.

Entre sus principales funciones estarán:

- Ejecutar las tareas de seguridad de la información que le asigne el gerente de la cooperativa.

- Monitorear las violaciones de seguridad y aplicar acciones correctivas para asegurar que se provea la seguridad adecuada.
- Preparar y monitorear el programa de concientización en seguridad para todos los colaboradores y partes interesadas del sistema de gestión de seguridad de la Información de la cooperativa FAVI UTP.
- Probar la arquitectura de seguridad para evaluar la fortaleza de la seguridad y para detectar las posibles amenazas.
- Definir la estrategia de gestión de los riesgos de seguridad de la información, coordinar su implementación y centralizar el monitoreo sobre su ejecución.
- Coordinar la identificación y evaluación de los riesgos de seguridad de la información a los cuales están expuestos los activos de la cooperativa, para identificar y aplicar el plan de tratamiento más adecuado.
- Coordinar la implementación de acciones correctivas y planes de tratamiento de riesgos del sistema de seguridad en la Información con los respectivos responsables, de acuerdo con los resultados de los diagnósticos realizados.
- Gestionar la actualización del sistema de gestión de seguridad en la Información.
- Supervisar el cumplimiento de los procedimientos del sistema de gestión de seguridad de la Información.
- Promover la creación, actualización de las políticas de tercer nivel, estándares de seguridad de la información y velar por el cumplimiento de las mismas.
- Apoyar la consolidación de la cultura de seguridad de la información a todos los funcionarios y partes interesadas del sistema de gestión de seguridad en la Información de la cooperativa FAVI UTP.
- Participar activamente en las actividades convocadas por la gerencia.
- Coordinar la realización periódica de diagnósticos internos y pruebas de vulnerabilidad de acuerdo con las políticas establecidas y requerimientos regulatorios.
- Elaborar y proponer ante la gerencia, procedimientos y controles para el mejoramiento del sistema de gestión de seguridad en la Información.
- Proponer a la gerencia y a la coordinación de educación y promoción, planes de capacitación y entrenamiento para difundir las políticas, normas y estándares de seguridad de la información al personal.
- Apoyar y coordinar el desarrollo de actividades de investigación y búsqueda de información referente a seguridad de la información.
- Elaborar los informes que le sean requeridos por la gerencia sobre el sistema de gestión de seguridad en la Información.
- Implementar y hacer seguimiento al plan de mejoramiento continuo del sistema de gestión de seguridad en la Información.
- Apoyar en los procesos de certificación y mantenimiento en el tiempo del sistema de gestión de seguridad de la Información.

Nota: para el desarrollo del análisis de riesgo de seguridad de la información, se deberá emplear la GUÍA METODOLÓGICA DE ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

7. Políticas

7.1 Política de primer nivel de sistema de seguridad de la información

La cooperativa FAVI UTP busca ser la mejor aliada financiera de sus asociados, colaboradores y comunidad objetivo, generando soluciones innovadoras, de calidad, basadas en sus principios y valores cooperativos, que cumplan con los requisitos legales y organizacionales suscritos frente al sistema de gestión de seguridad de la información integrado y dando cumplimiento a las normas establecidas en materia de seguridad de la información según el alcance establecido y en concordancia a los lineamientos vigentes de la norma NTC – ISO – IEC 27001 en su versión 2013, se compromete a:

1. Asegurar la confidencialidad, integridad y disponibilidad de la información de la cooperativa FAVI UTP, así como la información de sus asociados y terceros en su poder; acorde con el nivel de riesgo aceptado por la cooperativa.

2. Gestionar los riesgos en seguridad de la información que facilite la identificación, valoración, implementación de controles, monitoreo y seguimiento de los niveles de riesgos.

3. Mantener y evaluar el Sistema de gestión de seguridad de la Información.

Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

7.2 Políticas de tercer nivel del sistema de gestión de seguridad de la información para la mitigación del riesgo.

La coordinación de sistemas analiza y evalúa los riesgos asociados a sus activos de información, de acuerdo con la Guía metodológica de análisis de riesgos de seguridad y privacidad de la información con código A05GAR, al mismo tiempo que implementan planes de tratamiento que permitan gestionar los riesgos de seguridad y privacidad de la información.

a. Los colaboradores de la cooperativa deben tener conocimiento de los posibles riesgos, causas y vulnerabilidades asociados a cada activo de información con los que interactúan en función de sus actividades laborales, esto con el fin de propender por garantizar los principios de confidencialidad, integridad y disponibilidad de la información.
b. La Alta Dirección promueve la ejecución de las acciones correctivas asociadas a la prevención de los riesgos para la seguridad de la información.
c. La revisión de los riesgos de seguridad de la Información se llevará a cabo como mínimo una vez al año.

7.3 *Políticas de tercer nivel de sistema de seguridad de la información para Dispositivos Móviles*

La cooperativa establece para los casos cuando la cooperativa es custodio o propietario de los dispositivos móviles, como equipos portátiles, teléfonos móviles y/o tabletas se deben implementar controles de acceso y otros controles como los siguientes:

a. Se debe tener cifrado el almacenamiento para preservar la confidencialidad en caso de pérdida.
b. La red a la que se conectan los dispositivos móviles deberá tener controles de acceso y segregación.
c. Se identifican y autentican los dispositivos específicos antes de establecer cualquier tipo de conexión a recursos informáticos de la cooperativa
d. La coordinación de sistemas define los mecanismos de autorización para la conexión de dispositivos móviles que no son de su propiedad y que necesiten hacer uso de sus recursos.
e. Se debe reportar a control interno la pérdida o robo del dispositivo móvil en caso de tener servicios de la cooperativa configurados en el mismo.

7.4 Políticas de tercer nivel de sistema de seguridad de la información para el teletrabajo y trabajo remoto

La cooperativa establece las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la cooperativa; así mismo, suministra las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

Teletrabajo

a. La coordinación de sistemas coordinara la implementación de los recursos tecnológicos necesarios para uso de esta modalidad de trabajo dado el caso de que se llegara a implementar en un futuro, puesto que actualmente no se ejerce teletrabajo dentro de la cooperativa. Además,

debe disponer los métodos y controles de seguridad para establecer las conexiones remotas respectivas.

Acceso Remoto

a. La coordinación de sistemas debe restringir las conexiones remotas a los recursos de los recursos tecnológicos; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
b. La coordinación de sistemas debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos tecnológicos de la cooperativa de manera permanente.
c. Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos tecnológicos de la cooperativa y deben acatar las condiciones de uso establecidas para dichas conexiones.
d. Los usuarios deben usar recursos seguros para establecer la conexión remota.

7.5 Políticas de tercer nivel de sistema de seguridad de la información para el control y administración de accesos

La cooperativa FAVI debe controlar el acceso de la información y restringirla solo al personal autorizado conforme el perfil de acceso, teniendo en cuenta mecanismos de protección para la red y la información, así mismo garantiza la implementación de controles de perímetros de seguridad para la protección de áreas con instalaciones de procesamiento de información y cualquier otra área considerada crítica para la operatividad de la cooperativa.

a. Son usuarios de la red de la cooperativa FAVI todos los colaboradores, los trabajadores en misión, los contratistas, los pasantes y terceros, bien sea personas naturales o empresas que estén de forma temporal o permanente en la cooperativa.
b. El acceso a la red por parte de proveedores debe ser solicitado al coordinador de sistemas.

Requisitos adicionales

a. La cooperativa FAVI debe revisar las cuentas de los sistemas de información, una vez al año.
b. La cooperativa utiliza mecanismos para apoyar la administración de cuentas del sistema de información y servicios de TI

c. La cooperativa debe utilizar mecanismos para auditar las acciones de creación y desactivación de cuentas y notificar a los usuarios en la medida en que se requiera.

7.6 Políticas de tercer nivel de sistema de seguridad de la información para control de acceso a redes

Para tener acceso a cualquier red de la cooperativa, los colaboradores, contratistas y demás personas deben cumplir los siguientes lineamientos:

a. La conexión a las redes de la cooperativa se debe hacer de manera segura.
b. La coordinación de sistemas, para dar acceso a la utilización de la red inalámbrica debe capacitar a los usuarios e informar sobre los riesgos asociados al uso de esta tecnología.
c. No podrán tener acceso a la red inalámbrica de la cooperativa, usuarios y equipos no autorizados.

7.7 Políticas de tercer nivel de sistema de seguridad de la información de seguridad para internet

El acceso a Internet deberá ser utilizado con propósitos autorizados o con el destino por el cual fue provisto. La coordinación de sistemas debe definir los procedimientos para solicitar y aprobar accesos a Internet. Así mismo, se deben definir las pautas de utilización de Internet para todos los usuarios.

a. Acceder a Internet por el canal contratado y aprobado por la cooperativa. No se autoriza hacer conexiones no controladas ni limitadas hacia Internet como es el caso del uso de proxys o VPN.
b. Brindar el acceso de acuerdo con los perfiles de navegación definidos por la cooperativa.
c. Toda conexión deberá estar protegida por un firewall y deberá realizarse a través del router principal de la cooperativa.
d. Los colaboradores deberán abstenerse de navegar en sitios de juegos en línea, redes sociales, pornografía, terrorismo, hacktivismo y cualquier categoría que esté fuera del contexto laboral y/o que infrinja la normatividad aplicable.
e. Las conexiones directas desde equipos institucionales salida a internet no están permitidas.
f. Adicionalmente, la cooperativa FAVI como administrador de la red de Internet, podrá deshabilitar los permisos de acceso a internet en el momento en que lo considere necesario y más aún cuando la seguridad de la información haya sido comprometida.
g. La coordinación de sistemas podrá monitorear el correcto uso de los recursos de acceso a internet cuando lo considere necesario.

7.8 Políticas de tercer nivel de sistema de seguridad de la información sobre el uso de controles criptográficos

La cooperativa FAVI debe utilizar técnicas de cifrado para la protección de la información de acuerdo con las exigencias normativas y su criterio o criticidad de la información a cifrar. Se han definido los siguientes lineamientos, orientados a:

a. Los sistemas de información deben implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares y guías aplicables.
b. Proporcionar una protección adecuada a los equipos utilizados para generar, almacenar y archivar claves, considerándolos críticos o de alto riesgo.
c. Proteger las claves secretas y privadas evitando sean copiadas o modificadas sin autorización.
d. Se deben establecer procedimientos respecto a la administración de claves y el restablecimiento de llaves dañadas con el fin de que se garantice la confidencialidad de la clave.
e. Los colaboradores deberán dar el uso y protección adecuada a los mecanismos criptográficos asignados por la Entidad.

7.9 Políticas de tercer nivel de sistema de seguridad de la información de protección de llaves criptográficas

Para la cooperativa FAVI, las claves criptográficas son un activo de información que permite proteger la confidencialidad e integridad de la información, garantizando así que tanto el emisor como el receptor de la información, envían y reciben información fidedigna, veraz e íntegra, por tal razón la cooperativa deberá propender por:

a. Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
b. Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
c. Los colaboradores de la cooperativa deben aplicar los controles necesarios para evitar accesos no autorizados a las llaves criptográficas asignadas.

7.10 Políticas de tercer nivel de sistema de seguridad de la información de seguridad física y del entorno

Se deben implementar mecanismos de control de acceso físico para el personal y terceros para permitir el acceso a las instalaciones y áreas seguras de la cooperativa, solo al personal autorizado con el objetivo de salvaguardar de la

información, los equipos de cómputo, comunicaciones y demás activos de información de la cooperativa**.**

- Las áreas de procesamiento de información, centros de cableado, racks de comunicaciones deben estar protegido con mecanismos de control de acceso físico.
- Los visitantes deben ser acompañados por el coordinador o practicante de sistemas que avala el ingreso, durante el tiempo que dure la visita.
- Se debe restringir el ingreso de mascotas a la cooperativa, salvo en el caso de mascotas de acompañamiento (perros guías).

7.11 Políticas de tercer nivel de sistema de seguridad de la información de escritorio limpio y pantalla limpia

Se debe adoptar por parte de la cooperativa una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

a. Se debe guardar bajo llave o bajo algún nivel de seguridad según corresponda, los documentos en papel, dispositivos removibles o cualquier tipo de información clasificada o reservada generada o custodiada por la cooperativa.
b. Al finalizar la jornada de trabajo, los colaboradores de la cooperativa guardan en un lugar seguro los documentos y dispositivos removibles que contengan información clasificada o reservada de la cooperativa.
c. El uso de fotocopiadoras, escáner, fax o cualquier medio en que se puedan generar copias o difundir información hacia afuera de la cooperativa es manejado solamente por los colaboradores, con el fin de proteger la información de personal externo a la cooperativa.
d. Los colaboradores deben mantener bajo su custodia los documentos enviados a los equipos de impresión evitando que estos documentos queden desatendidos sobre la impresora u otro lugar.
e. Los colaboradores deben eliminar los documentos digitalizados del repositorio de documentos escaneados tan pronto como sean generados evitando que estos documentos previniendo la fuga de información.
f. Cuando el colaborador de la cooperativa se retire de su sitio de trabajo deberá bloquear su sesión personal evitando comprometer información.

7.12 Políticas de tercer nivel de sistema de seguridad de la información de controles contra códigos maliciosos

La cooperativa debe proporcionar los mecanismos necesarios que propendan por la protección de la información y la plataforma tecnológica y esto incluye el procesamiento y almacenamiento de información, minimizando los riesgos asociados, además de evitar divulgación, modificación o daño permanente por la filtración de software malicioso. Así mismo se debe generar conciencia entre los colaboradores, contratistas y personal externo a la cooperativa sobre la importancia de la seguridad de la información y los ataques por código malicioso.

a. Instalar y actualizar periódicamente el software de detección de malware, para analizar computadores, dispositivos móviles, removibles o cualquier otro dispositivo conectado a la red de la cooperativa.
b. Mantener los sistemas de seguridad de la información actualizados, por parte del área de coordinación de sistemas o quien corresponda.
c. Se debe contar con una herramienta que permita verificar la presencia de virus en archivos recibidos de fuentes externas o a través de redes no confiables.
d. Concienciar a los colaboradores de la cooperativa sobre la importancia de verificar el remitente de la información y de los riesgos asociados a los virus que pueden conllevar.
e. Los usuarios deben reportar a la coordinación de sistemas cualquier evento sospechoso que pudiera vulnerar la seguridad de la información.

7.13 Políticas de tercer nivel de sistema de seguridad de la información respaldo de la información

Son aplicables los procedimientos de copias de seguridad vigentes de los sistemas de información, los cuales deben estar almacenados en un medio diferente de donde reside la información original con el fin de asegurar la integridad y disponibilidad de la información, de la siguiente manera:

a. La información contenida en los servidores se respalda de forma periódica, discriminando las bases de datos de los sistemas de información, backup de los sistemas de información, sistemas de seguridad informática e información de los usuarios.
b. La retención de la información debe estar definida por los dueños de la información que está contenida en cada uno de los sistemas de información o acorde con la normatividad aplicable.
c. Las copias de seguridad son probadas periódicamente para garantizar la integridad de la información almacenada y que pueda ser recuperada oportunamente, el tiempo de recuperación varía de acuerdo con la información que se está respaldando.
d. Para garantizar que la información de los colaboradores, contratistas y demás terceros autorizados sea respaldada, es responsabilidad de cada usuario mantener copia de la información que se maneje en el recurso compartido dentro del file server de la cooperativa.

e. Los colaboradores, contratistas y/o terceros deben almacenar la información clasificada y reservada que gestionan en el recurso compartido definido para cada área dentro del file server de la cooperativa.
f. Los medios de almacenamiento con información crítica o copias de respaldo son manipulados única y exclusivamente por el personal encargado de hacer los respaldos y su salvaguarda.
g. La carpeta donde el colaborador y/o contratista guarda la información calificada como pública debe estar sincronizada con la carpeta compartida del servidor, para garantizar la disponibilidad de la información en todo momento.

7.14 Políticas de tercer nivel de sistema de seguridad de la información para la instalación de software

a. Los colaboradores de la cooperativa no deben instalar ningún programa o software.
b. Las instalaciones y/o actualizaciones de los programas vigentes en la cooperativa deben ser realizadas o autorizadas por la coordinación de sistemas siendo está área la única que puede realizarlas.
c. En el caso de los dispositivos móviles o portátiles de los cuales es propietaria la cooperativa, los funcionarios no deben instalar ningún software, programa o aplicativo en los equipos designados para su labor en la cooperativa.

7.15 Políticas de tercer nivel de sistema de seguridad de la información para la transferencia de la información

La cooperativa FAVI debe asegurar la protección de la información en el momento de ser trasferida o intercambiada con otras entidades o partes externas y establecer los procedimientos que permitan mantener la integridad, confidencialidad y disponibilidad de la información. Además, debe instaurar el *"Acuerdo de Confidencialidad y Reserva de Manejo de la Información"* entre contratistas y la cooperativa, por otra parte, se deben utilizar los mecanismos que permitan la transferencia de forma confiable, sin embargo, se deben definir directrices para él envió de información en medio físico o por un dispositivo de almacenamiento externo.

a. No se debe enviar información clasificada o reservada de la cooperativa a personal externo sin conocimiento previo del jefe inmediato o el responsable de la custodia de la información.
b. El envío de cualquier tipo de información se debe hacer por medio del correo electrónico institucional.
c. Está prohibido el uso del correo electrónico personal para el envío o recepción de cualquier tipo de información relacionada con la cooperativa.

7.16 Políticas de tercer nivel de sistema de seguridad de la información de desarrollo seguro

La cooperativa FAVI, debe velar porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Por tanto, establece los siguientes requerimientos:

a. Se deben tener ambientes de desarrollo, pruebas y producción.
b. El Coordinador de sistemas define los permisos necesarios de acceso a los ambientes.
c. Los requerimientos de seguridad de la información se deben incluir y verificar en todo el ciclo de vida del desarrollo del software.
d. Se deben restringir el acceso a los repositorios de códigos fuentes de programa.
e. Se deben mantener control de versionamiento del código fuente dentro del proyecto.
f. Se deben realizar pruebas que validen y verifiquen las vulnerabilidades en el desarrollo del proyecto.
g. Se deben tener en cuenta los estándares de codificación sugeridos por la industria de desarrollo y adoptarlos de manera pertinente a los proyectos.
h. El coordinador de sistemas debe utilizar las herramientas necesarias para apoyar la revisión del código del proyecto.
i. Cuando el proyecto es contratado externamente, el proveedor debe garantizar que las condiciones de seguridad descritas en esta política se cumplan en su totalidad.

7.17 Políticas de tercer nivel de sistema de seguridad de la información para las relaciones con proveedores

Los proveedores, contratistas y demás personal externo que trabaje para la cooperativa FAVI deben velar por la disponibilidad, confidencialidad e integridad de la información a la cual tengan acceso durante la permanencia en las instalaciones de la cooperativa, para tal fin se establecen las siguientes condiciones:

a. Los proveedores o contratistas que tengan relaciones comerciales con la cooperativa deberán firmar el *Acuerdo de Confidencialidad y Reserva de manejo de la Información*.
b. Los proveedores deben tener acceso sólo a la información de la cooperativa requerida para su labor.
c. Para el ingreso a áreas seguras, los proveedores o contratistas, deben estar permanentemente acompañados de personal de la cooperativa y cumplir con los controles establecidos.

7.18 Políticas de tercer nivel de sistema de seguridad de la información para la gestión de incidentes de seguridad de la información.

La cooperativa, debe hacer una adecuada gestión de los incidentes que se generen dentro de la organización, de acuerdo con la anterior premisa la cooperativa establece que:

a. Las partes interesadas del sistema de seguridad en la Información deben reportar oportunamente la información del incidente a los niveles apropiados.
b. Todos los colaboradores, contratistas y terceros de los sistemas y servicios de información deben notificar y/o reportar cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios que son utilizados en la cooperativa.
c. Todos los incidentes de seguridad reportados serán gestionados y se les hará seguimiento por parte del coordinador o practicante de sistemas.
d. La coordinación de sistemas y las áreas pertinentes deben evaluar los eventos de seguridad de la información y tomar decisiones sobre ellos.
e. Se debe documentar el aprendizaje obtenido de los incidentes de seguridad de la información, de igual manera se debe tener en cuenta el tratamiento realizado para la gestión de incidentes anteriores, los cuales serán tenidos en cuenta para ser evaluados como posibles soluciones para incidentes futuros en la cooperativa.
f. Se debe llevar un registro de los incidentes de seguridad de la información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

7.19 Políticas de tercer nivel de sistema de seguridad de la información para la gestión de continuidad del negocio

La cooperativa debe implementar un Plan de Continuidad de Negocio, con la finalidad de mitigar el impacto de los incidentes de interrupción, en los cuales la cooperativa no tiene injerencia directa, para lo cual se establecen las siguientes acciones que permiten recuperar la operación de esta:

a. Se debe establecer un Plan de Continuidad del Negocio con el fin de restaurar la operación, después de la ocurrencia de un incidente de interrupción mayor.
b. Los Planes de Recuperación de Desastres de la cooperativa, deben ser probados una vez al año, por la coordinación de sistemas con la participación de las áreas pertinentes; con el fin de verificar la efectividad de los mismos e identificar la mejora continua del proceso.

7.20 Políticas de tercer nivel de sistema de seguridad de la información de derechos de la propiedad intelectual

La cooperativa FAVI debe garantizar que el software que adquiera y usa la cooperativa, se encuentra debidamente licenciado, considerando y acatando los derechos de propiedad intelectual; además establece:

a. La cooperativa cumple con la reglamentación de propiedad intelectual para lo cual debe implementar los controles necesarios que garanticen el respeto de dicha reglamentación.
b. No se debe permitir el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por los derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.
c. Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de estos, con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
d. Se deben conservar pruebas y evidencias de propiedad de las licencias.
e. Se debe dar cumplimiento con los términos y condiciones establecidos para obtener software e información en redes públicas.
f. Se debe hacer un control sobre el uso de software libre que hacen los usuarios, y su relación con la función que realizan.
g. El software desarrollado internamente por el personal que labora en la cooperativa es propiedad exclusiva de la cooperativa, al igual que sus documentos, planos, diseños, esquema y otros desarrollos con medios de la cooperativa o por medio de terceros desarrollados para fines del negocio.

El coordinador de sistemas o quien haga sus veces, autorizará la utilización de software catalogado como libre, OpenSource o con licencias públicas (GPL), teniendo en cuenta que no se vea afectado de ninguna manera la cooperativa.

7.21. Políticas de tercer nivel de sistema de seguridad de la información para el manejo de correo electrónico

La cooperativa mediante la coordinación de sistemas establece los siguientes mecanismos para la gestión segura del correo electrónico:

Consideraciones generales:

- La cuenta de correo electrónico que pone a disposición de los colaboradores y contratistas únicamente podrá ser utilizada para finalidades relacionadas

con el desarrollo de las funciones correspondientes al cargo o función, quedando limitado el uso de dicha cuenta al ámbito laboral y profesional.

- Los usuarios no deben utilizar una cuenta de correo electrónico que pertenezca a otra persona. En caso de ausencias o vacaciones, se debe recurrir a mecanismos alternos como redirección de mensajes.
- Cualquier correo electrónico sospechoso debe ser reportado a *soporte@faviutp.com o cooperativa@faviutp.com*
- Los colaboradores, contratistas que tengan atribuida la gestión de cuentas de correo genéricas asociadas a determinados trámites no podrán en ningún caso hacer uso de ellas por motivos personales.
- Toda la información almacenada, gestionada o transmitida por correo electrónico de la cooperativa, es propiedad de la misma.
- Cuando se realice el envío de información clasificada o reservada mediante correo electrónico, se deben tener en cuenta medidas de seguridad como el cifrado.
- El correo electrónico no podrá ser utilizado para enviar ni para contestar mensajes o cadenas de mensajes que pudiesen causar congestión en la red de la cooperativa, o que puedan introducir códigos maliciosos o materializar riesgos de seguridad en los sistemas de información e infraestructura tecnológica.

Creación de cuenta de correo:

- La coordinación de sistemas es la dependencia encargada de proveer acceso al correo electrónico a los usuarios autorizados.
- Las cuentas de usuario deben ser creadas basadas en el área del colaborador de la siguiente manera: funcion@faviutp.com

Solicitud de copias de respaldo de cuenta de correo:

- La solicitud de la copia de respaldo de una cuenta de correo electrónico que haya sido dado de baja, ya sea por retiro del funcionario o por terminación del contrato en caso de los contratistas, debe contar con la autorización escrita (correo electrónico o memorando), por parte de un funcionario con alguno de los siguientes cargos dentro de la cooperativa: Gerencia, coordinación de sistemas, esto con el fin de salvaguardar la integridad de la información y dar cumplimiento a las políticas de seguridad de la cooperativa.

Imagen Institucional

Con el fin de fortalecer la imagen institucional la cooperativa determina las siguientes características para los mensajes de correo electrónico:

- Fuente: Arial o Calibri
- Tamaño de fuente: 12 pts.
- Color de fuente: Negro

- Color de fondo: Blanco
- Firma institucional para con los estilos ya establecidos para nuevos correos, respuestas y envíos.

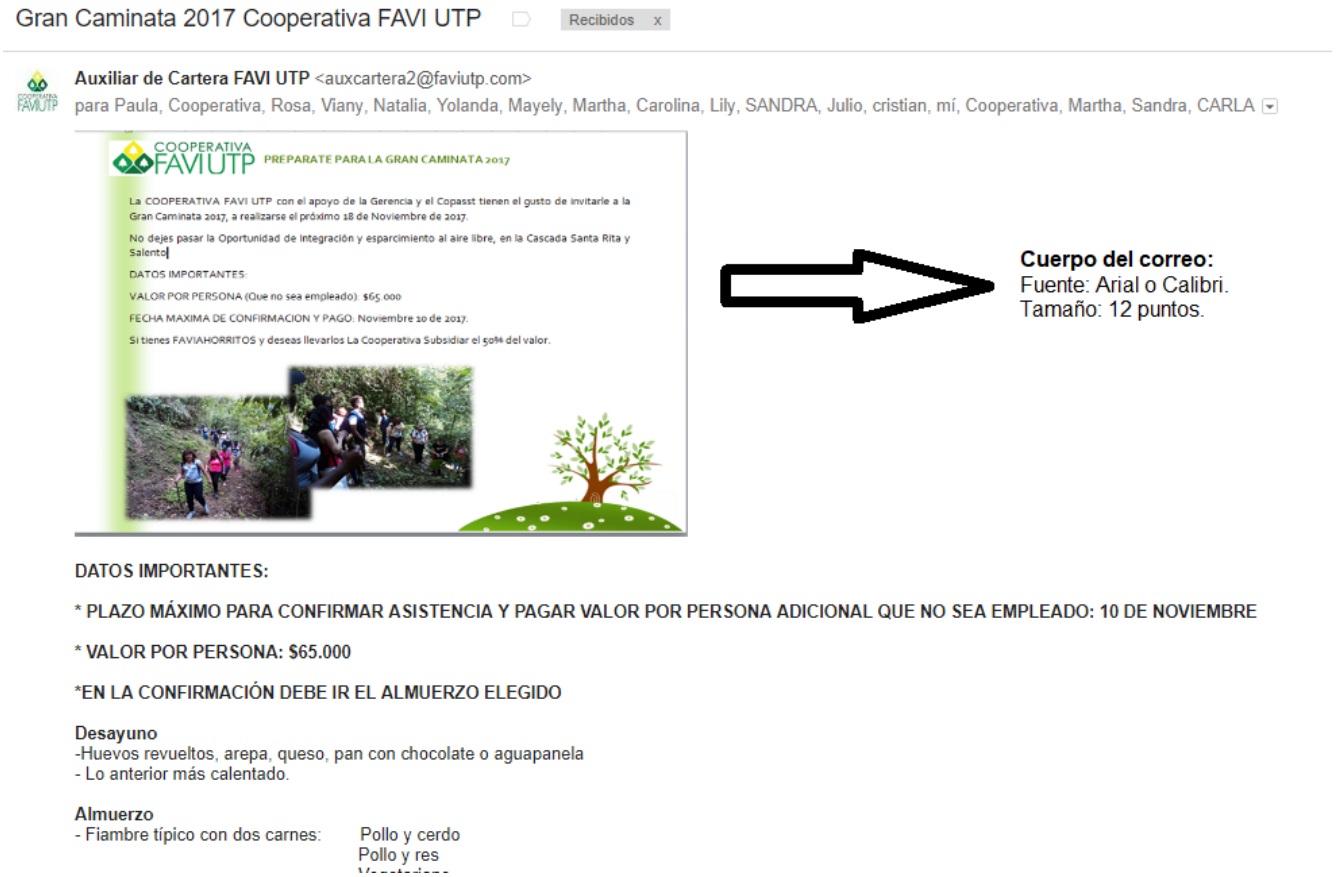


Figura # 21 Cuerpo del correo institucional

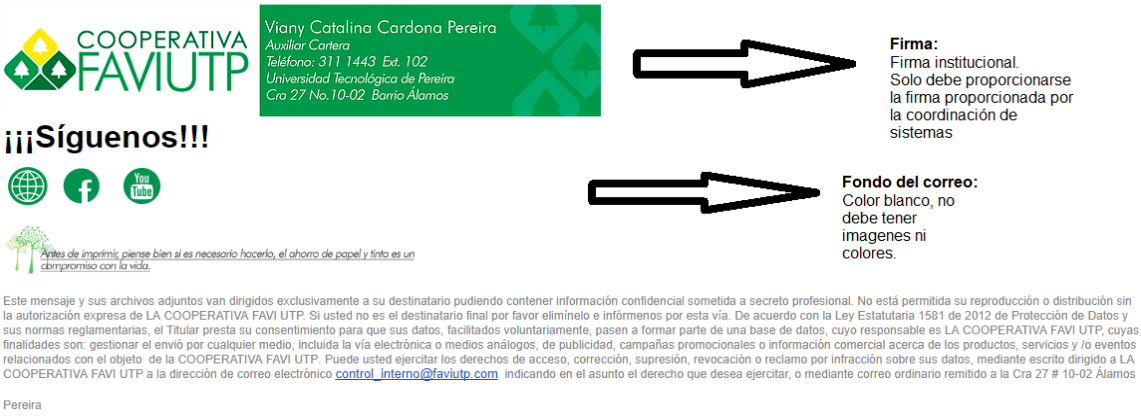


Figura # 22 Firma institucional

8. Política para protección de datos

La cooperativa FAVI UTP busca ser la mejor aliada financiera de sus asociados, colaboradores y comunidad objetivo, generando soluciones innovadoras, de calidad, basadas en sus principios y valores cooperativos, que cumplan con los requisitos legales y organizacionales suscritos frente al sistema de gestión de seguridad de la información integrado y dando cumplimiento a las normas establecidas en materia de seguridad de la información según el alcance establecido y en concordancia a los lineamientos vigentes de la norma NTC – ISO – IEC 27001 en su versión 2013, se compromete a:

1. Regular la recolección, almacenamiento, uso, circulación y eliminación de datos personales de nuestros usuarios.
2. Establecer procesos y lineamientos para el tratamiento de datos personales apoyándose en el sistema de seguridad de la información y en la gestión de activos de información.
3. Dar cumplimiento a lo establecido en la Ley 1581 de 2012, mediante la cual se expidió el Régimen General de Protección de datos personales, y demás normas que adicionen, modifiquen o deroguen la protección de datos personales.

4. Dar a conocer a todos nuestros usuarios los derechos y deberes que se derivan de la protección de datos personales.

5. Realizar socialización, divulgación y capacitación de los procesos y lineamientos establecidos para el tratamiento de datos personales a los funcionarios de la cooperativa FAVI a través del equipo conformado por la coordinación de sistemas para la implementación del sistema de seguridad de la Información.

6. Recolectar, actualizar y registrar la información que reposa en base de datos personales y está sujeta a tratamiento de la presente política.

7. Solicitar autorización a los usuarios titulares de la información, para su recolección, almacenamiento, uso, cesión, transmisión y eliminación.

Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar la implementación, seguimiento y evaluación de esta política.

9. Cumplimiento

El incumplimiento de las medidas definidas en las presentes políticas da lugar a la aplicación de las medidas administrativas, disciplinarias o legales a que haya lugar.

GUÍA METODOLÓGICA DE ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN COOPERATIVA FAVI UTP

1. OBJETIVO

Definir la metodología de gestión de riesgos de seguridad y privacidad de la información contemplando: Identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo en la cooperativa FAVI UTP, teniendo en cuenta los lineamientos descritos en la Norma Técnica Colombiana NTC-ISO/IEC 31000.

Realizar un análisis y valoración de los riesgos de seguridad de la información en cuanto al impacto y la probabilidad de ocurrencia para la cooperativa FAVI UTP.

Identificar las medidas de protección y remediación que contribuyan al correcto tratamiento de los riesgos a través de una adecuada selección y relación de controles informados en el Anexo A de la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 y los cuales contribuyan al cumplimiento de los objetivos de cada proceso y procedimiento evaluado

2. ALCANCE

La guía metodológica de análisis de riesgos de seguridad y privacidad de la Información provee los mecanismos necesarios para identificar, analizar, evaluar y tratar de manera adecuada los riesgos asociados a los activos de información de la cooperativa FAVI UTP.

3. ÁMBITO DE APLICACIÓN

La presente guía aplica para el sistema integrado de gestión de la cooperativa FAVI UTP.

4. REQUISITOS DE CALIDAD APLICABLE

Está guía da cumplimiento a los lineamientos establecidos en la Norma NTC-ISO/IEC 27001[1]

5. DEFINICIONES

Los siguientes términos y definiciones que se encuentran en el presente documento están Basados en la Norma NTC-ISO/IEC 27000, ISO 31000, GTC 137 (ISO Guía

[1] Debe tenerse en cuenta el último versionamiento para trabajar

73:2009), GTC ISO 27035 y son aplicables al sistema integrado de gestión de la cooperativa FAVI UTP.

Para una mejor comprensión de la presente guía metodológica, se toman como referencia los términos y definiciones establecidos en la Norma NTC-ISO/IEC 27000, Norma NTC-ISO/IEC 27005, Norma NTC-ISO/IEC 31000 y la guía práctica para la consolidación del componente de administración de riesgos A05GCR del proceso de políticas de seguridad de la información de la cooperativa FAVI UTP.

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.
Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.
Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
Autenticidad: Propiedad de que una cooperativa es lo que afirma ser.
Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones. La revelación no autorizada de la información calificada de acuerdo con un nivel de confidencialidad alto implica un grave impacto en la cooperativa FAVI, en términos económicos, de su imagen y ante sus clientes.
Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma técnica NTC-ISO/IEC 27001:2013.
Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los asociados de la cooperativa FAVI.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.
Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros: pérdida de reputación, implicaciones legales, etc.
Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la cooperativa FAVI debe ser clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información puede exponer a la empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.
Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
Probabilidad: Medida para estimar la ocurrencia del riesgo.
Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.
Responsable de Seguridad Informática: En la cooperativa FAVI la coordinación de sistemas será el encargado de realizar el seguimiento y monitoreo al Sistema de Gestión de la Seguridad de la información (SGSI).
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.
SGSI: Sistema de Gestión de la Seguridad de la Información.
Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
Valoración del riesgo: Proceso de análisis y evaluación del riesgo.
Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. VALORACIÓN DE RIESGOS EN EL CONTEXTO DE LA COOPERATIVA FAVI UTP ASOCIADOS A LOS ACTIVOS DE INFORMACIÓN

6.1. Contexto de la cooperativa FAVI UTP

La cooperativa FAVI busca ser la mejor aliada financiera de sus asociados, colaboradores y comunidad objetivo, generando soluciones innovadoras, de calidad, basadas en sus principios y valores cooperativos, cumpliendo los requisitos legales y organizacionales suscritos frente al Sistema Integrado de Gestión, en materia de administración de los riesgos institucionales y los de corrupción.

6.2. Contexto Interno

Lineamientos y programas:

- **GESTIÓN ESTRATÉGICA Y ADMINISTRATIVA**

Posicionamiento Organizacional. Fortalecer la capacidad de gestión organizacional a través del desarrollo de competencias de los órganos de dirección y ejecución para el logro de la excelencia de la cooperativa, apoyados en una cultura de planeación.

- **INTERMEDIACIÓN FINANCIERA**

Servicio al Asociado y Portafolio de Servicios. Facilitar las operaciones en los diferentes servicios en forma confiable, oportuna e innovadora, contribuyendo con

él con el cumplimiento de las disposiciones, normas, protección de los activos y valor agregado a la prestación del servicio.

- **DESARROLLO ACADÉMICO**

Formación, Capacitación, Emprendimiento e Innovación. Contribuir en el crecimiento y desarrollo del conocimiento de los asociados, colaboradores y la comunidad, la formación del pensamiento financiero y cooperativo, fortaleciendo sus ideas y proyectos.

- **COMPROMISO Y PARTICIPACIÓN ACTIVA PARA PROMOVER EL MODELO COOPERATIVO.**

Apoyo a las redes tecnológicas y de servicios promovidas por el sector solidario. Fortalecer la capacidad económica del movimiento cooperativo a nivel regional, nacional e internacional.

Oferta de Productos y Servicios:

- **AHORRO A LA VISTA**

Es un depósito ordinario a la vista, en el cual los fondos depositados por él cual tienen disponibilidad inmediata y le generan rentabilidad diaria durante el periodo del depósito de acuerdo con el monto ahorrado. El Ahorro a la Vista se define como el ahorro a la orden, disponible y manejado a través de documento idóneo.

- **AHORRO PROGRAMADO**

Los depósitos de Ahorro Programado se definen como un convenio de ahorro entre la Cooperativa y el asociado, mediante el cual éste último se compromete a depositar unas cuotas periódicas determinadas durante un plazo establecido, por lo que la Cooperativa reconoce una tasa de interés pactada.

- **AHORRO A TÉRMINO (CDAT)**

Permiten ahorrar dinero a un término fijo, generando intereses. La tasa de interés puede ser superior a la tasa de las cuentas de ahorros y por ello son más atractivos. Los CDAT pueden transferirse por endoso y se diferencian de los CDT en que pueden abrirse a un plazo menor de 30 días, que es el plazo mínimo de los CDT.

- **FAVI AHORRITO**

Es un depósito a la vista en pesos, con liquidez inmediata que genera intereses sobre saldos diarios, con el fin de enseñar a los niños desde la edad temprana a manejar su dinero e incentivar la cultura del ahorro. Diseñada para los hijos de los asociados hasta que cumplan los 18 años.

- **CONSUMO CUPO ROTATIVO**

Es un cupo de crédito que la Entidad asigna a los asociados, de acuerdo con la capacidad de endeudamiento y a la historia crediticia, con el propósito de que el asociado disponga de manera ágil y oportuna de los recursos, utilizando para ello, las redes de cajeros electrónicos y puntos de pago de las entidades.

- **CONSUMO COMPRA DE CARTERA EXTERNA**

Crédito dirigido a la compra de cartera de las tarjetas de crédito cuyo plazo máximo será de treinta y seis (36) meses, con pago por libranza, contratación de planta y/o jubilados sin deudor hasta los montos estipulados por el reglamento de crédito.

- **CONSUMO CON ORDENES DE COMPRA**

Destinado exclusivamente a órdenes de compras para ser utilizadas en los establecimientos que tienen convenio vigente con la Cooperativa. Se establece una cuantía máxima de Tres salarios mínimos legales mensuales vigentes (3 SMLMV), con un plazo no superior a cuatro (4) meses.

- **CONSUMO ESTUDIO**

Se otorgará para estudios técnicos o tecnológicos, pregrado y posgrado, en instituciones educativas, debidamente reconocidas, para el pago de la matrícula del asociado o su grupo familiar, entendiéndose por este el conyugue, compañero(a) permanente, los hijos, y personas que dependan económicamente del asociado. El desembolso se girará a la entidad educativa con base en el comprobante de liquidación.

- **CONSUMO NUEVAS TASAS**

Créditos para asociados con contratación a término indefinido y/o jubilados, con un cupo máximo de diez (10) veces el salario, y un plazo hasta de seis (6) años con pago por libranza y sin deudor solidario. Para asociados con contratos a término fijo el plazo será el de la duración del contrato.

- **PRESTACIONES SOCIALES**

Es el crédito que puede pactarse en una cuota de pago. En esta modalidad se pueden incluir o comprometer: primas de servicios, bonificaciones laborales, prima de vacaciones, prima navideña, bonificación por servicios, mesada adicional de junio, mesada adicional de diciembre, prestaciones sociales por liquidación de contrato entre otras. Esta línea de crédito podrá ser utilizada.

- **CONSUMO GARANTÍA REAL**

Su monto es hasta el valor cubierto por la compañía de seguros, con un plazo de hasta seis (6) años, y requiere constitución de garantía real.

- **CRÉDITO LÍNEA DE VEHÍCULO (FAVI-AUTO)**

Destinado para compra de vehículo. Cupo 90% del valor Comercial o valor de la factura, para vehículo nuevo. 80% del menor valor Fasecolda o comercial hasta 5 años. Interés 1.2% MV, hasta 60 meses, si el vehículo nuevo o hasta 48 meses, si el vehículo es usado.

- **TURISMO, RECREACIÓN Y SALUD**

Destinado exclusivamente para programas de recreación o plan de turismo y salud. El monto máximo del crédito será de 1 hasta 100 S.M.M.L.V. Interés 1.3% N.M. hasta 48 meses.

- **CONSUMO CON CODEUDOR**

Son aquellos créditos que otorga La Cooperativa, exigiendo como garantía un deudor solidario, el cual deberá cumplir con las condiciones señaladas en el reglamento. Plazo máximo de Seis (6) años. El monto máximo del crédito será hasta el valor cubierto por la compañía de seguros.

- **CRÉDITO INMEDIATO**

Se otorgará con un plazo no superior a 12 meses, con un interés del 1.4% nominal mensual o 18.16% EA, su monto depende del salario que devengue el asociado según la tabla. Se puede cancelar realizando consignación o descuento por nómina en las fechas de corte de la UTP, diligenciando la respectiva autorización por escrito.

- **CRÉDITO DE CONSUMO**

Son órdenes de compras con un plazo de cuatro (4) meses para ser utilizadas en los establecimientos con los cuales el FAVI UTP tiene convenio.

- **CRÉDITO POR CALAMIDAD**

Destinado exclusivamente para financiar casos de calamidad por Salud que no cubra la EPS de acuerdo con el reglamento del Fondo de Solidaridad. Su cuantía será hasta 4 (cuatro) SMMLV, con un plazo hasta 18 (dieciocho) meses; dos (2) meses muertos sin intereses para los asociados, los cuales serán cubiertos por el fondo de solidaridad.

- **CRÉDITO LÍNEA DE APORTES-LIBRE DESTINACIÓN**

Se presta hasta 5 veces el monto de lo que tenga en aportes sociales con un plazo de hasta 72 meses. (Tasa el 0.95% Nominal mensual).

- **BENEFICIOS**

Ser codueño de su Cooperativa FAVI UTP. Seguro de vida gratuito por $5.400.000. Revalorización de sus Aportes. Brinda protección y previsión gratuita, con el plan exequial LA OFRENDA S.A. Capacitación, integración y recreación. Auxilios de Solidaridad cuando el asociado presente una calamidad. Acceso amplio al portafolio integral de servicios.

- **CONVENIOS COMERCIALES**

Coomeva Medicina Prepagada. Telefonía Celular – claro. Multident. EMI. Visual Moderna. Gimnasio Lina López NT Native Tongue Instituto de Inglés Canadiense. Almacén Alkosto. Almacenes Éxito. Club de Patinaje Fenix Perla del Otún. Red Médica Vital. Liceo Altair

6.3. Contexto con los Grupos de Interés

- **Alta Dirección de la Cooperativa FAVI UTP:**
  Requisitos en Sistema de Seguridad de la Información: Implementar el Sistema de Seguridad de la Información para preservar la disponibilidad, confidencialidad y disponibilidad de la información de la cooperativa.
  Expectativas en Sistema de Seguridad de la Información: Mitigar los riesgos que puedan afectar la Seguridad de la Información de la cooperativa.

- **Funcionarios(Colaboradores) de la Cooperativa FAVI UTP:**
  Requisitos en Sistema de Seguridad de la Información: Mantener disponible la información de la cooperativa FAVI para poder cumplir con las labores asignadas en el menor tiempo posible. De igual manera proteger la información personal de cada funcionario de acuerdo con lo establecido en la Ley 1581 de 2012.
  Expectativas en Sistema de Seguridad de la Información: Garantizar la continuidad de las operaciones de la Cooperativa FAVI UTP, mantener la integridad de los datos generados en las operaciones diarias de la cooperativa.

- **Asociados de la cooperativa:**
  Requisitos en Sistema de Seguridad de la Información: Dar buen uso a los datos personales y demás información que se suministre para adelantar un proceso de cualquier índole dentro de la cooperativa.
  Expectativas en Sistema de Seguridad de la Información: Asegurar por parte de la cooperativa una adecuada prestación de los servicios hacia ellos.

- **Proveedores:**
  Requisitos en Sistema de Seguridad de la Información: Cumplir con los acuerdos contractuales.
  Expectativas en Sistema de Seguridad de la Información: Garantizar la disponibilidad de los sistemas de información para poder cumplir con el objeto contractual estipulado.

- **Coordinación de Sistemas de la cooperativa:**
  Requisitos en Sistema de Seguridad de la Información: Cumplimiento a cabalidad de las normas establecidas como lo son la ISO IEC 27001:2013.
  Expectativas en Sistema de Seguridad de la Información: Que se cree una cultura de Seguridad de la información en la cooperativa, de tal manera que cada funcionario sea consciente de la importancia de la información que maneja, además, proteger a la cooperativa de los riesgos informáticos a los que se ve expuesta, mitigar los impactos de la ocurrencia de la materialización de los riesgos.

6.4. Comunicación

A medida que se desarrollan las acciones del proceso de Análisis de Riesgos de Seguridad y Privacidad de la Información, la comunicación se realiza para mantener informada a la dirección, la o las dependencias involucradas con la gestión del riesgo y el equipo o grupo de trabajo encargado de la implementación del Sistema de Gestión de Seguridad de la Información; igualmente recibir información de los procesos y las partes interesadas. De esta manera, se consigue difundir la información necesaria para obtener el consenso de los responsables y los afectados por las decisiones sobre el tratamiento de los riesgos.

Las acciones de comunicación son importantes para:

- Identificar los riesgos.
- Valorar los riesgos en función de las consecuencias para el negocio y la probabilidad de ocurrencia.
- Comprender la probabilidad y consecuencias de los riesgos.
- Establecer prioridades para el tratamiento de riesgos.
- Informar y contribuir a que se involucren las partes interesadas.
- Monitorear la efectividad del tratamiento de los riesgos.
- Revisar con regularidad el proceso y su monitoreo.
- Concienciar a la entidad y a la dirección sobre los riesgos y su forma de mitigarlos.

6.5. Contexto de Seguridad y Privacidad de la Información

La información de la cooperativa FAVI UTP sin importar el tipo, es crucial para el desarrollo de su objeto misional, su correcto desempeño dentro de la política interna y su relación con el asociado es por ello por lo que debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad de la información y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la cooperativa.

De acuerdo con lo anterior y tomando como referencia el Modelo de Seguridad y Privacidad de la información de MINTIC[2] (MSPI), la gestión de riesgos de seguridad y privacidad de la información en la cooperativa FAVI UTP utiliza las buenas prácticas de las Norma Técnica Colombiana (ISO/IEC 31000, ISO/IEC 27005), la "Guía de Riesgos" del DAFP[3] e integrando con lo que se ha desarrollado al interior de la entidad para otros modelos de Gestión (por ejemplo SGC[4]), aprovechando el trabajo adelantado en la identificación de riesgos por el actual coordinador de sistemas para ser complementados con los riesgos de seguridad y privacidad de la información.

[2] Ministerio de Tecnologías de la Información y de las Comunicaciones (MINTIC).

[3] Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP).

[4] Sistema de Gestión de Calidad (SGC)

El Procedimiento (A05PAR[5]) de Administración de Riesgos de la cooperativa FAVI UTP, tiene como objetivo administrar los riesgos institucionales mediante la identificación, clasificación, evaluación, valoración y seguimiento de los mismos con el fin de prevenir y mitigar los eventos generados por su materialización; su alcance inicia con la identificación del contexto estratégico de la cooperativa, continúa con la clasificación, evaluación y valoración, y finaliza con el seguimiento de la política de administración de riesgos y aplica para todos los procesos y Sistema de Gestión.

7. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1. Definición del Riesgo

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias". De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información de la cooperativa FAVI UTP.

De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital[6], la estrategia de administración de riesgos para el flujo de la información en los procesos de la cooperativa FAVI, busca diseñar una metodología ágil enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información:

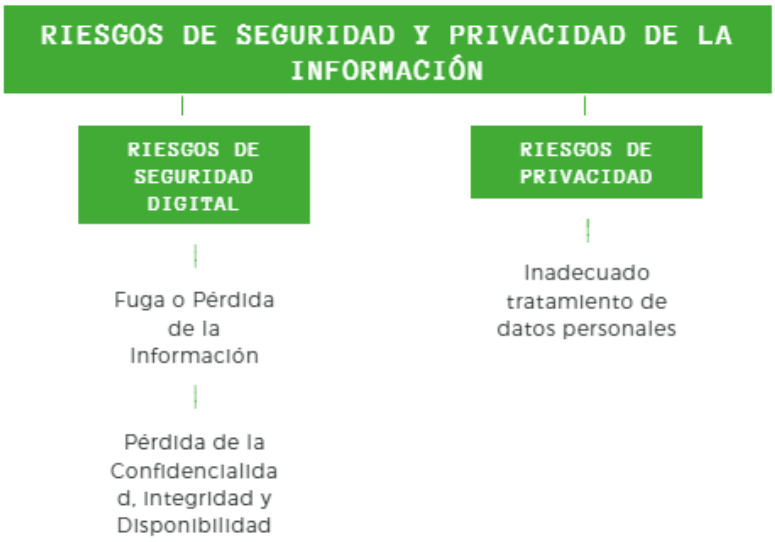


Figura # 23 Riesgos de Seguridad y Privacidad de la Información

[5] Procedimiento de Administración de Riesgos A05PAR de la cooperativa FAVI UTP

[6] Departamento Nacional de Planeación. CONPES 3854

7.2. Riesgos de Seguridad Digital

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico[7]. En la tipificación de dichos riesgos, se encuentran los siguientes:

a. **Fuga o Pérdida de la Información:** Información que hace que esta llegue a personas no autorizadas, sobre la que su responsable pierde el control o el estado que genera una condición irreparable en el tratamiento y procesamiento de la Información. Ocurre cuando un sistema de información o proceso diseñado para restringir el acceso sólo a sujetos autorizados revela parte de la información que procesa o transmite debido a errores en la ejecución de los procedimientos de tratamiento, las personas o diseño de los Sistemas de Información.
b. **Pérdida de la Confidencialidad:** Violación o incidente a la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.
c. **Pérdida de la Integridad:** Pérdida de la propiedad de mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
d. **Pérdida de la Disponibilidad:** Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

7.3. Riesgos de Privacidad

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos. Como riesgo tipificado se cuenta con **Inadecuado Tratamiento de Datos Personales:** Uso no adecuado de la información que identifica a las personas, lo que repercute en una violación de los derechos constitucionales.

7.4. Incidente de Seguridad de la Información

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como “Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y vulnerar la seguridad”; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información.

[7] Departamento Nacional de Planeación. CONPES 3854.

7.5. Id. Riesgo

Los riesgos serán identificados de acuerdo con las tres iniciales del nombre del proceso, seguido de la letra “R” y el número consecutivo.

7.6. Factores de Riesgo

Se entiende por factores de riesgo dentro del Sistema de Gestión de Seguridad de la Información, aquellos que pueden afectar la confidencialidad, la integridad o la disponibilidad de la información de la cooperativa FAVI. Entre los factores de riesgos que se encuentran identificados dentro de la cooperativa están los siguientes:

Factor de Riesgo	Descripción
Personas	Personal de la organización que se encuentra relacionado con la ejecución del proceso de forma directa o indirecta.
Procesos	Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
Tecnología	Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la cooperativa.
Factores Externos	Condiciones generadas por agentes externos, las cuales no son controlables por la cooperativa y que afectan de manera directa o indirecta el proceso.

Tabla # 1 Factores de Riesgo asociados al SGSI

8. METODOLOGÍA DE ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA FAVI UTP

8.1. Metodología de Valoración del Activo y Análisis de Riesgos de Seguridad de la Información

La Cooperativa FAVI UTP utiliza una metodología para valorar los riesgos de la Seguridad de la Información, basado en los sistemas de gestión que se encuentran en fase de implementación. La presente Guía Metodológica y la Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyen al Sistema de Gestión abarcando los siguientes aspectos:

a. Se identifican los activos de información en el flujo de cada proceso, teniendo en cuenta las Tablas de Retención Documental, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociada a los factores.

En el esfuerzo de valoración del activo, se consideran los siguientes aspectos:

TIPO DE ACTIVOS	DESCRIPCIÓN
Activos Esenciales	**Datos importantes o vitales para la Administración de la Cooperativa:** Aquellos que son esenciales, imprescindibles para la continuidad de la cooperativa; es decir que su carencia o daño afectaría directamente a la cooperativa, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). **Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	**Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.** Ejemplo: Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba.
Hardware / Infraestructura	**Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la cooperativa, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo,

	Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (vhost), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.
Software / Aplicaciones Informáticas	**Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.** Ejemplo: Desarrollo Inhouse, Desarrollo Subcontratado, Estándar, Navegador, Servidor de Presentación (www), Servidor de Aplicaciones (app), Cliente de Correo Electrónico, Servidor de Correo Electrónico, Servidor de Ficheros (file), Sistemas de Gestión de Bases de Datos (dbms), Monitor Transaccional, Ofimática, Antivirus, Sistema Operativo (OS), Servidor de Terminales, Sistema de Backup o Respaldo, Gestor de Máquinas Virtuales.
Servicios	**Funciones que permiten suplir una necesidad de los usuarios (del servicio).** Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Idcooperativaes (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos, PKI (Infraestructura de Clave Pública).
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
Soportes de Información	**Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo.** Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (rdsi).

Claves Criptográficas	**Esenciales para garantizar el funcionamiento de los mecanismos criptográficos.** Ejemplo: Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación.
Equipos Auxiliares	**Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.** Ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.

La Valoración del Activo de Información se realiza mediante la identificación del impacto para la cooperativa FAVI UTP por la pérdida de las propiedades, principios o fundamentos de la Seguridad de la Información, teniendo en cuenta la siguiente tabla de criterios:

Criterio	Valor
Crítico	**= 5**
Alto	**= 3 y < 5**
Medio	**= 1 y < 3**
Bajo	**= 0 y < 1**

Tabla # 2 Criterios

CONFIDENCIALIDAD: Impacto que tendría para la cooperativa FAVI, la pérdida de confidencialidad sobre el activo de información, es decir, que sea conocido por personas no autorizadas:

- **5. Crítico:** Es la existencia de información más crítica (Calificada, Vital o Esencial) a nivel de pérdida de su confidencialidad que cualquier otra y que por ende debe tener una mayor protección. A la información (Calificada, Vital o Esencial) sólo pueden tener acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente a la cooperativa.
- **4. Alto:** Es la información que es utilizada por los funcionarios de la cooperativa para realizar sus labores en los procesos y que no puede ser

conocida por terceros sin autorización del propietario del activo. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al proceso evaluado y/u otros procesos de la cooperativa.

- **3. Medio:** Es la información que es utilizada por los funcionarios de la cooperativa para realizar sus labores en los procesos y que puede ser conocida por terceros con la autorización del propietario del activo. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al proceso evaluado y/u otros procesos de la cooperativa.
- **2. Bajo:** Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada con ciertas restricciones dadas por el propietario del activo a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos de la cooperativa. El conocimiento o divulgación no autorizada de la información que gestiona este activo no tiene ningún impacto negativo en los procesos de la cooperativa.
- **1. Mínimo:** Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos de la cooperativa. El conocimiento o divulgación no autorizada de la información que gestiona este activo no tiene ningún impacto negativo en los procesos de la cooperativa.
- **0. Nulo:** Es la información que ha sido calificada como de conocimiento público y su divulgación no implica impacto negativo en los procesos de la cooperativa.

INTEGRIDAD: Impacto que tendría la pérdida de integridad, es decir, si la exactitud y estado completo de la información y métodos de procesamiento fueran alterados.

- **5. Crítico:** La pérdida de exactitud y estado completo del activo impacta negativamente la prestación de servicios de tecnología y de información en la cooperativa.
- **4. Alto:** La pérdida en la exactitud de algún dato o estado del activo impacta negativamente la prestación de servicios de tecnología y de información en la cooperativa.
- **3. Medio:** La pérdida posible en la exactitud de algún dato o estado completo del activo puede impactar negativamente al proceso que gestiona la información y/o a otros procesos de la cooperativa.

- **2. Bajo:** La pérdida posible en la exactitud de algún dato o estado completo del activo puede tener algún impacto negativo en los procesos de la cooperativa.
- **1. Mínimo:** La pérdida de exactitud y estado completo activo no tiene ningún impacto negativo en los procesos de la cooperativa.
- **0. Nulo:** La pérdida de exactitud y estado no genera situación negativa alguna en los procesos de la cooperativa.

DISPONIBILIDAD: Impacto que tendría la pérdida de disponibilidad, es decir, si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran.

- **5. Crítico:** La falta o no disponibilidad de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en la cooperativa.
- **4. Alto:** La falta o no disponibilidad parcial de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en la cooperativa.
- **3. Medio:** La falta o no disponibilidad de algún dato que posea el activo de información o el mismo impacta negativamente al proceso que gestiona la información y/o a otros procesos de la cooperativa.
- **2. Bajo:** La falta o no disponibilidad del activo de información en su componente puede tener algún impacto negativo en los procesos de la cooperativa.
- **1. Mínimo:** La falta o no disponibilidad del activo de información no tiene ningún impacto negativo en los procesos de la cooperativa.
- **0. Nulo:** La falta o no disponibilidad de algún dato que posea el activo de información no afecta los procesos de la cooperativa.

b. Se identifican los responsables y dueños de la información con base en la oficina o dependencia productora, así mismo se le asocian a su responsabilidad, el tratamiento de los riesgos de seguridad identificados.

c. Se consideran los factores de riesgo, las vulnerabilidades de los activos de información, las causas o amenazas que puedan determinar la materialización de un evento, sus posibles consecuencias o afectación, relacionándolos con la identificación del riesgo de seguridad o privacidad de la información. Todo lo anterior se realiza mediante la documentación de fuentes como: Entrevistas no estructuradas con los responsables de los activos y el desarrollo del flujo de la información en el proceso, fuentes estadísticas y tendencias de los riesgos de seguridad y privacidad, observaciones de expertos y analistas, estudio de los

procedimientos, guías y diagramas de información, establecimiento de la criticidad del activo y su tratamiento por parte de las personas, los procesos y la tecnología, gestión de riesgos realizados anteriormente y detección de áreas o dependencias sensibles.

d. Se determina la probabilidad de ocurrencia para cada riesgo teniendo en cuenta los siguientes criterios de valoración:

NIVEL	CONCEPTO	DESCRIPCIÓN	FRECUENCIA
1	**Rara Vez**	Puede que no se haya presentado u ocurrir solo en circunstancias excepcionales.	Nunca o no se ha presentado en los últimos 5 años
2	**Improbable**	Pudo ocurrir en algún momento, es poco común o frecuente	Al menos una vez en los últimos 5 años
3	**Posible**	Puede ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	**Probable**	Ocurrirá en la mayoría de las circunstancias.	Al menos una vez en el último año
5	**Casi Seguro**	Se espera que ocurra en la mayoría de las circunstancias	Más de una vez al año

Tabla # 3 Valoración de la Probabilidad de Ocurrencia

e. La valoración del impacto que puede ocasionar a la cooperativa FAVI, la materialización del Riesgo de Seguridad o Privacidad de la Información se representa con la descripción de los siguientes niveles:

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
1	**Insignificante**	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización	Afecta a una actividad del proceso.
2	**Menor**	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
3	**Moderado**	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.	Afecta un conjunto de datos personales o el proceso.
4	**Mayor**	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Afecta varios conjuntos de datos personales o procesos de la organización.

5	**Catastrófico**	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.	Afecta toda la organización. Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la organización.

Tabla # 4 Valoración del Impacto

Con base en la determinación de la probabilidad y la valoración del impacto, se establecen los niveles de riesgos teniendo una clasificación propia para la cooperativa FAVI:

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo Extremo	**Mayor o igual a 20**	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	**Mayor o igual a 15 y menor a 20**	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Riesgo Moderado	**Mayor o igual a 10 y menor a 15**	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
Riesgo Menor	**Mayor o igual a 5 y menor a 10**	Mitigar el riesgo mediante de medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.
Riesgo Bajo	**Menor a 5 y mayor a 0**	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.

Tabla # 5 Dimensión de Riesgos

Valoración del Riesgo: Se considera la probabilidad de que la amenaza identificada explote la vulnerabilidad y el impacto resultante sobre el activo evaluado, determina el Riesgo Total interpretado en las siguientes zonas de riesgo de acuerdo con el siguiente Mapa de Calor:

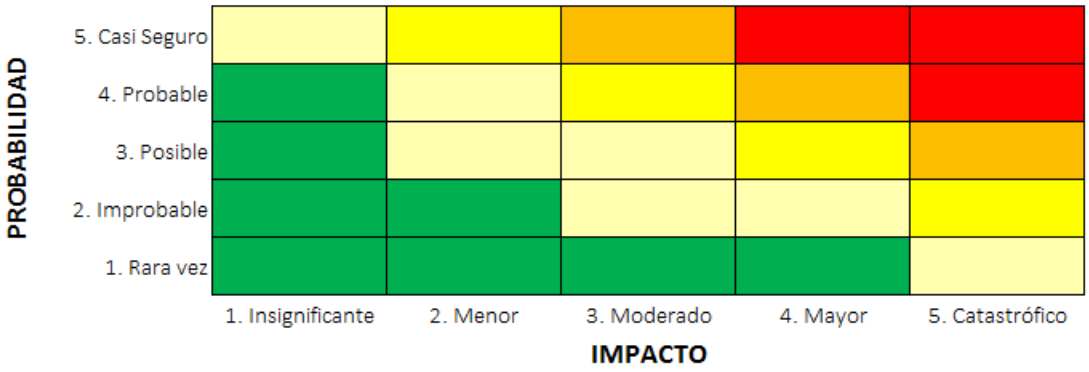


Figura # 24 Mapa de Calor para la Representación de los niveles de Riesgo por Zonas

En concordancia y alineación con los Niveles de Riesgos, las acciones requeridas se complementan en la siguiente tabla:

Zona de Riesgo Aceptable	**Asumir el Riesgo:** Riesgos para los cuales se determina que el nivel de exposición es adecuado y por lo tanto se acepta.
Zona de Riesgo Tolerable	**Mitigar el Riesgo:** Riesgos que se puede permitir gestionar, que en caso de materialización la cooperativa se encuentra en la capacidad de asumirlo.
Zona de Riesgo Moderado	**Mitigar o Evitar el Riesgo:** Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Importante	**Mitigar o Evitar el Riesgo:** Implementación de controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.
Zona de Riesgo Inaceptable	**Evitar el Riesgo:** Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

Tabla # 6 Zona de Riesgo

9. MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

9.1. Matriz de Riesgos y Seguridad de la Información – A05MAA

La documentación del registro de activos de información, su valoración en cuanto a las dimensiones de Confidencialidad, Integridad, Disponibilidad y el análisis de riesgos de seguridad y privacidad de la información, se realiza utilizando el formato Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad y Privacidad de

la Información, código A05MAA para lo cual se describe a continuación, el esquema de diligenciamiento:

Campo	Definición	Responsable de diligenciamiento
Dependencia / Dirección / Coordinación	Área o dependencia productora de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Proceso Asociado	Proceso Productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Objetivo Proceso	Objetivo del Proceso productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Procedimientos Asociados	Procedimientos que apoyan el Proceso Productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Objetivos Procedimientos Asociados	Objetivos de los procedimientos que apoyan el Proceso Productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Controles asociados al proceso (Alineado con NTC-ISO/IEC 27002)	Controles que se cumplen al cumplirse el desarrollo de los objetivos del Proceso Productor de la Información a través de la gestión en conjunto de los Activos de Información del Proceso Productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas

Figura # 25 Matriz de Riesgos de Seguridad y Privacidad de la Información – Encabezado de la Matriz.

Campo		Definición	Responsable de diligenciamiento
REGISTRO DE ACTIVOS DE INFORMACIÓN	PROPIETARIO / RESPONSABLE	Responsable del Proceso, del Activo de Información, de los Riesgos de Seguridad y Privacidad y de las Actividades de Tratamiento.	Dueño del proceso.
	S / Serie (Tema)	Codificación de la Serie Documental.	Coordinación de Sistemas
	CATEGORIA/SERIE	Nombre de la Categoría o Serie Documental.	Coordinación de Sistemas
	Sb / Subserie (Subtema)	Codificación de la Subserie Documental.	Coordinación de Sistemas
	Id. Activo	Codficación del Activo de Información (A), es consecutivo utilizado por la Coordinación de Sistemas para su fácil identificación. Cuando los activos de información son padres de varios activos, el identificador iniciará con el identificador del padre y luego se colocará el respectivo identificador. **Ejemplo:** Padre A1, hijos A1 Td, A2 Td y así sucecivamente.	Coordinación de Sistemas
	ACTIVOS DE INFORMACIÓN /SUBSERIE/Tipos Documentales	Nombre del Activo de Información. Trabajo en conjunto entre el dueño del proceso y Coordinación de Sistemas. La fuente inicial son las evidencias que seencuentran descritas en los documentos: Caracterización del proceso y los procedimientos asociados a esta caracterización. Los activos son validados con el dueño del proceso.	Dueño del proceso / Coordinación de Sistemas
	EL (Electrónico)	Electrónico de acuerdo a la definición Documental.	Coordinación de Sistemas
	SIG / Código Documento o Formato en Sistema de Gestión	Formato que hace parte del Sistema de Gestión.	Coordinación de Sistemas
	DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN	Descripción del Activo de Información, descripción que inicialmente se toma de la información relacionada en la caracterización y procedimientos asociados, y debe ser validada o en su defecto completada por el dueño del proceso.	Dueño del proceso / Coordinación de Sistemas
	Idioma	Idioma en el que se presenta el contenido de la Información. El dueño del proceso indica en qué idioma se encuentra la información que se maneja a través del activo de información que almacena la misma.	Dueño del proceso.
	MEDIO DE CONSERVACIÓN Y/O SOPORTE	Medio en el cual se presenta la información. Se toma directamente en lo establecido por la Ley 1712/2014.	Coordinación de Sistemas y Control Interno
	FORMATO	Formato en el cual se presenta la información. Se toma directamente en lo establecido por la Ley 1712/2014 y con validación del dueño de proceso.	Coordinación de Sistemas
	INFORMACIÓN PUBLICADA O DISPONIBLE	Si la información se encuentra de manera pública o disponible para su consulta.	Dueño del proceso.

Figura # 26 Matriz de Riesgos de Seguridad y Privacidad de la Información – Registro de Activos.

CALIFICACIÓN DE LA INFORMACIÓN	CONDICIÓN LEGÍTIMA DE LA EXCEPCIÓN	Condiciones que indican la selección de Calificación de la Información. Se toma directamente en lo establecido por la Ley 1712/2014.	Dueño del proceso.
	CONDICIÓN	Campo automático de acuerdo a la definición de la Condición legítima de la Excepción. Campo automático.	Coordinación de Sistemas
	CALIFICACIÓN (GGPD01 - GGFT01)	Categoría de Calificación de la Información. Campo automático.	Coordinación de Sistemas
VALORACIÓN DEL ACTIVO	TIPO DE ACTIVO	Identificación o categorización del tipo de activo. De acuerdo a la explicación de cada tipo de activo y se realiza una validación por parte de la Coordinación de Sistemas.	Dueño del proceso.
	CONFIDENCIALIDAD	Valoración de la Confidencialidad. Qué tan confidencial debe ser el activo de información que se está evaluando.	Dueño del proceso.
	INTEGRIDAD	Valoración de la Integridad. Qué tan íntegro en su contenido debe ser el activo de información que se está evaluando.	Dueño del proceso.
	DISPONIBILIDAD	Valoración de la Disponiblidad. Qué tan disponible para el público en general debe ser el activo de información que se está evaluando.	Dueño del proceso.
	DIMENSIÓN ACTIVO	Resultado final de la Valoración. Campo automático.	Coordinación de Sistemas
	OBSERVACIONES	Observaciones respecto al Activo de Información. Porqué se realizan esas calificaciones, y qué se tuvo en cuenta para determinar las mismas.	Dueño del proceso.
ANÁLISIS DE RIESGOS RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	FACTOR DE RIESGO	Principios que pueden afectar la confidencialidad, la integridad o la disponibilidad de la información.	Dueño del proceso.
	VULNERABILIDAD	Debilidad indentificada en el tratamiento del activo.	Dueño del proceso.
	CAUSA / AMENAZA	Oportunidades que pueden aprovechar las debilidades del activo.	Dueño del proceso.
	CONSECUENCIA / EFECTO	Resultado o desenlace del evento de riesgo.	Dueño del proceso.
	RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Riesgo identificado como parte del análisis de las anteriores variables. De acuerdo a la calificación realizada y alineada con los parámetros descritos en Guía A05GAR Guía Metodológica de Análisis de Riesgos de Seguridad y Privacidad de la Información.	Coordinación de Sistemas

Figura # 27 Matriz de Riesgos de Seguridad y Privacidad de la Información – Calificación, Valoración y Análisis de Riesgo para los Activos de Información.

VALORACIÓN DEL RIESGO INHERENTE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Id. Riesgo	Codificación del Riesgo. Consecutivo que brinda la coordinación de Sistemas para su fácil identificación en el momento que se requieran generar planes de tratamiento y seguimientos a los mismos.	Coordinación de Sistemas
	PROBABILIDAD	Posibilidad de ocurrencia del evento de riesgo.	Dueño del proceso.
	IMPACTO	Valoración de la consecuencia o efecto del evento de riesgo.	Dueño del proceso.
	DIMENSIÓN DEL RIESGO INHERENTE	Nivel resultante de la valoración de las anteriores variables. Campo automático.	Coordinación de Sistemas
	TIPIFICACIÓN DEL RIESGO	Categorización del Riesgo de Seguridad o Privacidad de la Información. Campo automático.	Coordinación de Sistemas
EFECTIVIDAD DE ACTIVIDADES O CONTROLES EXISTENTES	Descripción de la Actividad o Control Existente	Especificación de la Actividad o Control existente definida por el dueño del proceso.	Dueño del proceso.
	La Actividad o Control está documentada, cuenta con responsable	Verificación de la Documentación de la actividad o control existente definido por el dueño del proceso.	Dueño del proceso.
	La Actividad o Control se está Aplicando	Confirmación de la aplicación de la actividad o control existente defiido por el dueño del proceso.	Dueño del proceso.
	La Actividad o Control es Efectiva Cumple su función	Confirmación de la función de la actividad o control existente definido por el dueño del proceso.	Dueño del proceso.
	EFECTIVIDAD DE LA ACTIVIDAD O CONTROL EXISTENTE	Porcentaje de la efectividad de la actividad o control existente. Campo automático.	Dueño del proceso.
VALORACIÓN DEL RIESGO RESIDUAL	PROBABILIDAD	Posibilidad de ocurrencia del evento de riesgo luego de validar las actividades o controles existentes.	Dueño del proceso.
	IMPACTO	Valoración de la consecuencia o efecto del evento de riesgo luego de validar las actividades o controles existentes.	Dueño del proceso.
	DIMENSIÓN DEL RIESGO RESIDUAL	Nivel resultante de la valoración de las anteriores variables. Campo automático.	Coordinación de Sistemas
	TIPIFICACIÓN DEL RIESGO	Categorización del Riesgo de Seguridad o Privacidad de la Información. Campo automático.	Coordinación de Sistemas

Figura # 28 Matriz de Riesgos de Seguridad y Privacidad de la Información – Valoración de Riesgos Inherentes y Riesgos Residuales para los Activos de Información.

9.2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Con base en el resultado del análisis de riesgos de seguridad y privacidad de la información y con el fin de gestionar el riesgo residual, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de esta, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

El Plan de Tratamiento de Riesgos de Seguridad de la Información se integra a la presente Guía Metodológica y a la Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyendo al fortalecimiento de los mecanismos del Sistema Integrado de Gestión de la cooperativa FAVI UTP.

La formulación de actividades de tratamiento de riesgos de seguridad de la información y su aplicación de acuerdo con la valoración del riesgo inherente documentado, buscando integrar la implementación de la presente Guía Metodológica, describiendo a continuación, el esquema de diligenciamiento:

Dependencia / Dirección / Coordinación	Área o dependencia productora de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Proceso Asociado	Proceso Productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Objetivo Proceso	Objetivo del Proceso productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Procedimientos Asociados	Procedimientos que apoyan el Proceso Productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Objetivos Procedimientos Asociados	Objetivos de los procedimientos que apoyan el Proceso Productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas
Controles asociados al proceso (Alineado con NTC-ISO/IEC 27002)	Controles que se cumplen al cumplirse el desarrollo de los objetivos del Proceso Productor de la Información a través de la gestión en conjunto de los Activos de Información del Proceso Productor de la Información. Información que se extrae de la hoja A05MAA.	Coordinación de Sistemas

Figura # 29 Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Encabezado de la Matriz Plan de Tratamiento.

ANÁLISIS DE RIESGOS RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	RESPONSABLE	Quien debe liderar la ejecución y seguimiento de las actividades de tratamiento.	Dueño del proceso.
	ID RIESGO (A05MAA)	Identificador del riesgo de seguridad en la matriz de valoración de activos y analisis de riesgos de seguridad de la información, codigo A05MAA	Coordinación de sistemas.
	RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Nombre del riesgo de seguridad de la información resultante del analisis documentado en el formato A05MAA.	Coordinación de sistemas.
	DESCRIPCIÓN RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Analisis descriptivo del riesgo de seguridad identificado. Información que se extrae de la hoja A05MAA.	Coordinación de sistemas.
	VULNERABILIDADES	Listado de vulnerabilidades asociadas a la materializacion del riesgo de seguridad. Información que se extrae de la hoja A05MAA	Coordinación de sistemas.
	VALORACIÓN RESIDUAL	Nivel de riesgo en la valoración final, como producto del analisis del impacto y la probabilidad de ocurrencia, documentado en el formato A05MAA	Coordinación de sistemas.
	TRATAMIENTO	Decisión, frente a la accion de mitigación o tratamiento de la valoracion inherente. La coordinación de sistemas propone actividades para que sean evaluadas por el dueño del proceso.	Dueño del proceso.

Figura # 30 Tratamiento de Riesgos de Seguridad y Privacidad de la Información– Componentes de la Matriz Plan de Tratamiento.

TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	ACTIVIDADES DE TRATAMIENTO	Acciones encaminadas a lograr el tratamiento propuesto.	Dueño del proceso.
	RESPONSABLE	Quien debe liderar la ejecución y seguimiento de las actividades de tratamiento.	Dueño del proceso.
	RESPONSABLES ADICIONALES	Quien acompaña la ejecución y seguimiento de las actividades de tratamiento.	Dueño del proceso.
	RECURSOS TECNICOS	Recursos necesarios o propuestos para la implementación de las actividades de tratamiento y que estan integrados a a la adecuacion de los controles de seguridad de la información.	Dueño del proceso.
	RECURSOS DOCUMENTALES	Recursos procedimentales y guias requeridas, que apoyan y documentan las acciones y actividades de tratamiento de los riesgos de seguridad.	Dueño del proceso.
IMPLEMENTACIÓN DE ACTIVIDADES DE TRATAMIENTO	TIEMPO DE IMPLEMENTACIÓN	Tiempo estimado para la implementación de las actividades de tratamiento propuestas.	Dueño del proceso.
	FECHA MAXIMA DE IMPLEMENTACIÓN	Fecha limite de implementación de las actividades de tratamiento propuesto.	Dueño del proceso.
	VALORACIÓN RESIDUAL	Nivel de riesgo residual que se estima alcanzar al aplicar la decisión de tratamiento del riesgo residual.	Dueño del proceso.
	DECLARACIÓN DE APLICABILIDAD	Asociacion de los documentos normativos, procedimientos, guias y politicas que soportan el sistema de seguridad de la información y justifican la adecuacion de los controles de seguridad de acuerdo con la norma ISO 27001:2013.	Dueño del proceso.
	PORCENTAJE DE IMPLEMENTACIÓN	Avance de implementación de las actividades de tratamiento	Coordinación de Sistemas
	OBSERVACIONES	Información adicional o aclaratoria que aporta a la implementacion del plan de tratamiento propuesto.	Dueño del proceso.

Figura # 31 Tratamiento de Riesgos de Seguridad y Privacidad de la Información– Definiciones de Plan de Tratamiento.

10. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La cooperativa FAVI UTP “evaluará el desempeño del modelo de gestión de riegos de seguridad y privacidad de la información”, por medio de un monitoreo esencial para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo anual o en el momento que se determine, debe estar a cargo de los responsables de los procesos, la coordinación de Control Interno y la coordinación de Sistemas, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.[8]

[8] Procedimiento de Administración de Riesgos A05PAR de la Cooperativa FAVI UTP.

GUÍA
PRÁCTICA PARA LA CONSOLIDACIÓN DEL COMPONENTE DE ADMINISTRACIÓN DEL RIESGO

1. OBJETIVO

Establecer los conceptos básicos y metodológicos para la identificación, evaluación y gestión de aquellos eventos adversos, tanto internos como externos, que puedan afectar o impedir el logro de los objetivos de la cooperativa FAVI UTP.

2. ALCANCE

Inicia con el análisis del contexto estratégico, continúa con la identificación, análisis y valoración de los riesgos y finaliza con la consolidación de la política de administración de riesgos.

3. ÁMBITO DE APLICACIÓN

La presente guía aplica para todos los procesos del Sistema de Gestión y a la operación de la cooperativa.

4. DEFINICIONES

Acción: identificación y aplicación de las opciones de mejora para fortalecer los controles de los riesgos.
Análisis del riesgo: razonamiento que permite calificar y evaluar el riesgo inherente, en términos cualitativos y cuantitativos.
Administración de riesgos: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
Amenaza: situación externa que no controla la cooperativa y que puede afectar su operación.
Causa: medios, circunstancias y/o agentes que generan riesgos.

Control: acción que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

Control preventivo: acción orientada a eliminar las causas del riesgo para prevenir su ocurrencia o materialización.

Control correctivo: acción orientada a eliminar las causas del riesgo materializado para evitar que vuelva a ocurrir.

Debilidad: situación interna que la cooperativa puede controlar y que puede afectar su operación.

Evaluación del riesgo: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Identificación del riesgo: etapa en la que se determina el riesgo con sus causas y consecuencias.

Impacto: efecto de la materialización del riesgo.

Mapa de riesgos: documento que de manera sistemática muestra el desarrollo de las etapas de la administración del riesgo.

Opciones de manejo: posibilidades disponibles para administrar el riesgo (evitar, reducir, transferir o asumir el riesgo residual).

Plan de contingencia: documento que contiene el conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.

Probabilidad: medida para estimar la ocurrencia del riesgo.

Procedimiento: Conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

Proceso: Conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en los mismos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

Riesgo: eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

Riesgo inherente: eventualidad a la que se enfrenta una organización en ausencia de controles.

5. GENERALIDADES

Se hace necesario establecer un conjunto de elementos que le permiten a la cooperativa identificar, evaluar y gestionar aquellos eventos adversos, tanto internos como externos, que puedan afectar o impedir el logro de los objetivos.

6. PROCEDIMIENTO PARA LA ADMINISTRACIÓN DEL RIESGO

6.1 Selección información de entrada

Si bien el centro de la construcción del mapa de riesgos se enmarca en los procesos, es necesario tener en consideración la misión, visión, objetivos estratégicos de la cooperativa, los planes, así como los proyectos institucionales.

En cuanto a los procesos es necesario identificarlos a partir del mapa de procesos que ha sido definido para la cooperativa:

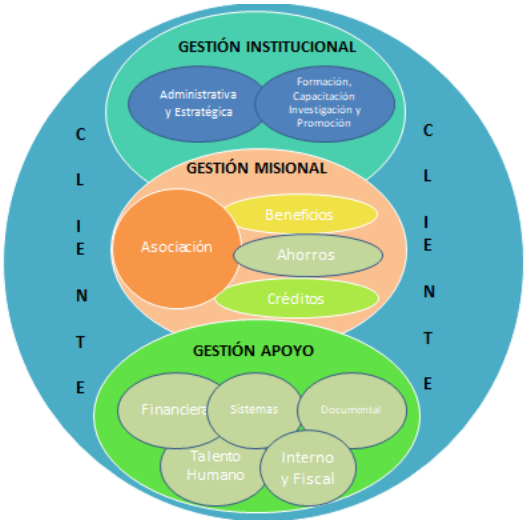


Figura # 32 Mapa de procesos Cooperativa FAVI UTP

6.2 Análisis Contexto Estratégico

Esta etapa corresponde al análisis de factores internos y externos que afectan la organización en cuanto a los procesos tecnológicos, en este sentido la presente metodología se centra en este último, es decir, el proceso. En tal sentido se utilizará como metodología la Matriz DOFA. Para su implementación se deberá tener en cuenta lo siguiente:

- **Matriz DOFA:** es un instrumento metodológico que sirve para identificar acciones viables, mediante el cruce de variables. El instrumento permite la identificación de acciones que potencien entre sí los factores positivos, así:

  - **Estrategias FO:** aprovechan las mejores posibilidades del entorno y las ventajas propias. Define una posición que permite la expansión de la organización y el fortalecimiento, para el logro de sus objetivos.
  - **Estrategias DO:** superan las debilidades internas, haciendo uso de las oportunidades que ofrece el entorno.
  - **Estrategias FA:** afrontan o evaden las amenazas del entorno, aprovechando las fortalezas de la organización.
  - **Estrategias DA:** disminuyen las debilidades internas y evitan las amenazas del entorno.
  - **Estrategias FD:** superan las debilidades utilizando las propias fortalezas.

	Fortalezas (I)	**Debilidades (I)**
	• Lista de fortalezas claves	• Lista de debilidades decisivas
Oportunidades (E)	**Estrategia FO**	**Estrategia DO**
• Lista de oportunidades claves	• Uso de fortalezas para aprovechar oportunidades	• Reducción de debilidades aprovechando oportunidades
Amenazas (E)	**Estrategia FA**	**Estrategia DA**
• Lista de amenazas relevantes	• Uso de fortalezas para enfrentar amenazas	• Reducción al mínimo de debilidades y control de amenazas

Figura # 33 Matriz DOFA

Tomando como referente lo anterior, se debe atender y seguir las siguientes orientaciones:

En la primera reunión se establecerán los factores internos y externos que afectan los procesos de sistemas. En una breve reunión se identificaron las siguientes fortalezas, debilidades, oportunidades y amenazas:

FORTALEZAS	• Trabajo en equipo entre áreas y sistemas • Interés y apoyo de la gerencia en optimizar la tecnología presente en la cooperativa • Coordinador de sistemas experimentado
DEBILIDADES	• Ausencia de documentación de procedimientos • Falta de capa • Falta de conocimiento y conciencia sobre seguridad de la información(capacitación) • No existen políticas en el uso de tecnologías documentadas • No hay políticas de retención de conocimiento y documentación cuando se generan soluciones a problemas en tecnología • Fallas persistentes de sistemas de impresión • Falla en el suministro eléctrico • Fallas imprevistas en los equipos • Fallas en el suministro de internet • Falta de definición y aplicación de controles para salvaguardar la información por parte de los funcionarios • Fallas en los servidores • Fallas en los canales de comunicación
OPORTUNIDADES	• Tercerización de servicios • Equipos de impresión multifuncionales

	• Aplicaciones de licencia libre • Cursos, tutoriales y videos en línea sobre herramientas tecnológicas y aplicaciones • Adopción de nuevas tendencias informáticas y uso de tecnologías
AMENAZAS	• Acelerado desarrollo tecnológico puede agilizar obsolencia de equipos • Sobrecosto por temas de mal uso de los equipos de impresión y por cultura de imprimir todo • Demanda creciente de los servicios ofrecidos • Seguridad de la información (virus y ataques informáticos) • Desconfianza de los asociados sobre el uso de su información o referente a la gestión tecnológica de la cooperativa

Para desarrollar lo expuesto y como parte introductoria se deberá informar a los asistentes, que, si una debilidad se da, se entenderá como algo desfavorable, carencia o que no se está haciendo bien, para lo cual deberán ser considerados como debilidades y/o amenazas:

- La administración, la estructura organizacional, las funciones y las responsabilidades.
- Las políticas, los objetivos y las estrategias que existen para su realización.
- Las capacidades, entendidas en términos de recursos y de conocimiento (humanos, de capital, tiempo, personas, infraestructura, procesos, sistemas y tecnologías).
- Los sistemas de información y comunicación, flujos de información formales e informales y toma de decisiones.
- Las normas, directrices y modelos adoptados por la organización.
- La forma y el alcance de las relaciones contractuales.

Las debilidades y/o amenazas deberán ser expresadas con términos similares a estos

Ausencia de….

…. obsoletos

Falta….

…insuficientes

Disminución de…

Fallas de….

Este tipo de palabras no necesariamente deben aparecer al inicio de la idea, ejemplo de estos, decir número de equipos de cómputo obsoletos

Al igual que las debilidades, los asistentes a la reunión deberán identificar estos aspectos desfavorables del entorno, para este caso puntual, no existe una regla específica de redacción, sin embargo, tendrán el mismo tratamiento de las debilidades, es decir afinidad por agrupación, generando como resultado un listado:

- Nueva tecnología disponible
- Nuevas leyes
- Incremento en el número de solicitudes por alta demanda de usuarios
- Poco conocimiento por parte de la ciudadanía
- Adaptación a normatividad internacional

En conclusión, esta etapa tiene como finalidad

- Identificar los factores externos que pueden ocasionar la presencia de riesgos, con base en el análisis de la información externa y los planes y programas de la cooperativa.
- Identificar los factores internos que pueden ocasionar la presencia de riesgos con base en el análisis y estudios sobre la cultura organizacional y clima laboral que se hayan adelantado en la cooperativa.

Conocidos los factores generadores de riesgo y dado por entendido que administrar los riesgos es un trabajo en equipo liderado y motivado constantemente por la Alta Dirección, se continúa con la identificación del riesgo.

Una vez estructurada la información se procederá a incluir la información (Proceso, Factores de Riesgo, Tipo de factor de riesgo y las Causas) en el formato.

Proceso	Contexto estratégico		
	Factores de riesgo	Tipo de factor de riesgo	Causas
CSIYC	Procesos Tecnología	Interno - Externo	1. Falta de conocimiento y conciencia sobre seguridad de la información 2. Falta de una adecuada capacitación para la toma de conciencia 3. Falla en los controles de seguridad informática 4. Carencia de herramientas de seguridad informática 5. Falta de plan de recuperación de desastres documentado, aprobado y materializado 6. Debilidad en la aplicación de la metodología de identificación de riesgos de seguridad de la información

Figura # 34 Contexto estratégico

6.3 Identificación de riesgos

Es el “elemento que posibilita conocer los eventos potenciales, estén o no bajo el control de la cooperativa FAVI, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia”

En este paso se identifican los riesgos de la cooperativa y por procesos que la organización debe gestionar. Esta identificación se realiza con base en el contexto estratégico, definido en el paso anterior.

Los riesgos por procesos parten del análisis del objetivo del proceso para identificar los eventos que puedan afectar su cumplimiento y los riesgos de la cooperativa parten de la identificación que hace la Alta Dirección de posibles eventos que, si se materializan, ponen en peligro el cumplimiento de la misión o la existencia misma de la organización. Estos eventos se identifican, mediante un análisis integral del contexto estratégico previamente definido.

Para la identificación de riesgos, suele utilizarse como metodología la denominada “Metalenguaje del riesgo”, el cual es un método apropiado para la definición de los riesgos consiste en usar el Metalenguaje específico para proveer una identificación del riesgo a través de tres preguntas:

- Debido a <una o más causas>,
- podría ocurrir <un riesgo>,
- lo que podría generar a <uno o más efectos>.

Con base en lo anterior, se presenta como ejemplo la siguiente expresión:

Debido a manejar con excesiva velocidad **podría ocurrir** un accidente **lo que podría generar** lesiones personales.
Esta estructura expresa:

Causa - riesgo - efecto

El metalenguaje del riesgo pretende asegurar que se identifiquen correctamente causas, riesgos y consecuencias, sin confundir unas con otras; de no ser así, los pasos posteriores quedan viciados de error.

De acuerdo con la etapa de contexto estratégico, se tomarán las causas establecidas para cada uno de los factores tanto internos, como externos, y además se tomará como ejemplo algunos factores internos de tecnología, talento humano y sistema de información:

FACTOR INTERNO	CAUSAS
1. Tecnología	1.1 Equipos insuficientes 1.2 Equipos obsoletos
2. Talento humano	2.1 Desconocimiento de la normatividad aplicada 2.2 Desmotivación 2.3 Resistencia al cambio
3. Sistemas de información	3.1 Información desactualizada

En este sentido, y para el primer factor tecnología, se identifican dos causas: equipos insuficientes y equipos obsoletos, analizando estas, se puede establecer un grado de afinidad, que permite tratarlas de manera conjunta, en tal sentido en la siguiente matriz:

DEBIDO A (Una o más causas)	PUEDE OCURRIR QUE (Riesgo)	DESCRIPCIÓN	LO QUE PODRÍA GENERAR (Uno o más efectos)

Las causas en este caso, que se les ha establecido cierto nivel de discapacidad, se incluirán en la celda DEBIDO A de la siguiente forma:

DEBIDO A (Una o más causas)	PUEDE OCURRIR QUE (Riesgo)	DESCRIPCIÓN	LO QUE PODRÍA GENERAR (Uno o más efectos)
• Equipos insuficientes • Equipos obsoletos			

Para el caso de talento humano, que cuenta con las siguientes causas

- Desconocimiento de la normatividad aplicada
- Desmotivación
- Resistencia al cambio

Se podrían encontrar dos grupos la primera en donde no se presenta afinidad y que se centra en la causa: desconocimiento de la normatividad aplicada y la otra que corresponde a la agrupación por afinidad de las causas: desmotivación y resistencia al cambio, estas al igual que las correspondiente a tecnología, se relacionan en la celda DEBIDO A, de otra parte, para el factor Sistema de

información, solo, cuenta con una causa, sin embargo esta no es ninguna limitante para incluirla en la matriz:

DEBIDO A (Una o más causas)	PUEDE OCURRIR QUE (Riesgo)	DESCRIPCIÓN	LO QUE PODRÍA GENERAR (Uno o más efectos)
• Equipos insuficientes • Equipos obsoletos			
• Desconocimiento de la normatividad aplicada			
• Desmotivación • Resistencia al cambio			
• Información desactualizada			

A pesar de que se agruparon causas del mismo factor, es necesario tener en cuenta que estas pueden unirse con causas de otros factores, es así como, en los casos analizados, podría encontrarse una afinidad entre causas de tecnología, con las de talento humano u otras, sin embargo, en algunos casos la afinidad puede establecerse en la siguiente fase del metalenguaje, que corresponde a la palabra “PUEDE OCURRIR QUE”, es decir cuando se identifica el riesgo.

Para iniciar la redacción del riesgo, se debe realizar el análisis de la totalidad de las causas inmersas en los factores internos y externos, previamente identificados, una vez estás han sido ubicadas en las respectivas casillas, se debe establecer, lo que puede ocurrir con estas causas, en este sentido esta reflexión se denominará riesgo, es necesario tener en cuenta que si bien pueden existir varias causas en una celda, siempre estás generarán un solo riesgo, para el primer grupo de causas: Equipos insuficientes y Equipos obsoletos, se deberá formular la siguiente pregunta, que puede ocurrir o generar si estas causas (LAS QUE ESTÁN EN LA CELDA DEBIDO A) se materializan, seguramente podría generar “*el incumplimiento en la generación de respuestas*

a los usuarios", lo mismo se hará con la segunda causa (o grupo de causas) y con las siguientes, para el ejemplo utilizado, el riesgo para cada grupo de causas es el siguiente:

DEBIDO A (Una o más causas)	PUEDE OCURRIR QUE (Riesgo)	DESCRIPCIÓN	LO QUE PODRÍA GENERAR (Uno o más efectos)
• Equipos insuficientes • Equipos obsoletos	incumplimiento en la generación de respuestas a los usuarios		
• Desconocimiento de la normatividad aplicada	incumplimiento en la generación de respuestas a los usuarios		
• Desmotivación • Resistencia al cambio	Generación de respuestas inadecuadas o erróneas a los usuarios.		
• Información desactualizada	Generación de respuestas inadecuadas o erróneas a los usuarios.		

Con base en la información relacionada, se identifica que varios grupos de causas provenientes de diferentes factores presentan un mismo riesgo, por lo que es necesario agruparlos alrededor de estos, también se debe tener en cuenta el nivel de afinidad, que, aunque no estén escritos de la misma forma, su esencia es exactamente la misma.

DEBIDO A (Una o más causas)	**PUEDE OCURRIR QUE (Riesgo)**	**DESCRIPCIÓN**	**LO QUE PODRÍA GENERAR (Uno o más efectos)**
• Equipos insuficientes • Equipos obsoletos	Incumplimiento en la generación		

• Desconocimiento de la normatividad aplicada	de respuestas a los usuarios		
• Desmotivación • Resistencia al cambio • Información desactualizada	Generación de respuestas inadecuadas o erróneas a los usuarios.		

Los riesgos deben ser descritos de modo tal que quien los lea, entienda cuál es su significado, en tal sentido, al frente de cada riesgo se colocará una breve explicación:

DEBIDO A (Una o más causas)	**PUEDE OCURRIR QUE (Riesgo)**	**DESCRIPCIÓN**	**LO QUE PODRÍA GENERAR (Uno o más efectos)**
• Equipos insuficientes • Equipos obsoletos • Desconocimiento de la normatividad aplicada	Incumplimiento en la generación de respuestas a los usuarios	No se generan las respuestas dentro de los Términos legales.	
• Desmotivación • Resistencia al cambio • Información desactualizada	Generación de respuestas inadecuadas o erróneas a los usuarios.	Respuestas sin la competencia técnica o no acorde a lo requerido.	

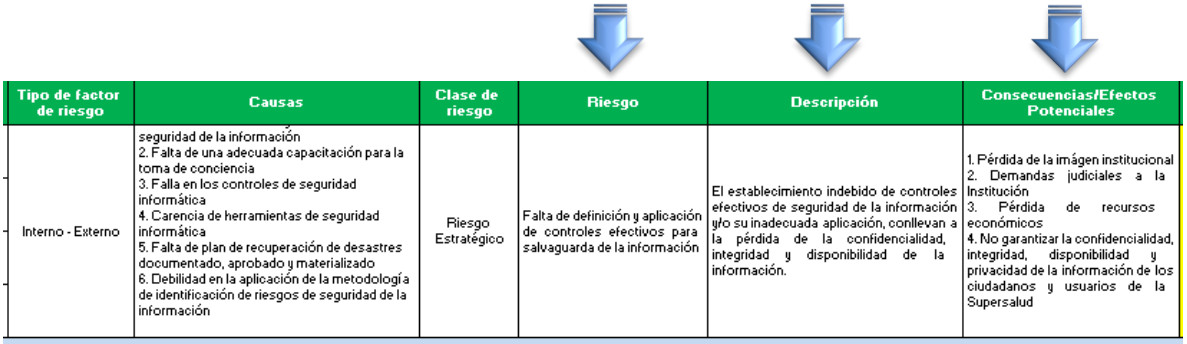
Teniendo claro los riesgos, se debe identificar el impacto que generaría la materialización del riesgo, en este sentido se puede presentar más de un efecto por riesgo, este impacto se establece respondiendo la expresión “LO QUE PODRÍA GENERAR”, para ello recuerde que:

DEBIDO A: XXXXXX PUEDE OCURRIR QUE YYYYY LO QUE PODRÍA GENERAR ZZZZ.

Para establecer el efecto se debe leer de manera seguida las tres expresiones enunciadas, es decir: Debido a, puede ocurrir que, y lo que podría generar, con esta información la matriz será complementada de la siguiente forma:

DEBIDO A (Una o más causas)	PUEDE OCURRIR QUE (Riesgo)	DESCRIPCIÓN	LO QUE PODRÍA GENERAR (Uno o más efectos)
• Equipos insuficientes • Equipos obsoletos • Desconocimiento de la normatividad aplicada	Incumplimiento en la generación de respuestas a los usuarios	No se generan las respuestas dentro de los Términos legales.	• Sanciones • Demandas
• Desmotivación • Resistencia al cambio • Información desactualizada	Generación de respuestas inadecuadas o erróneas a los usuarios.	Respuestas sin la competencia técnica o no acorde a lo requerido.	• Pérdida de imagen • Alto nivel de quejas por parte de los usuarios

Una vez estructurada la información se procederá a incluir la información (Riesgo, Descripción, Consecuencias/Efectos Potenciales) en el formato.



Tipo de factor de riesgo	Causas	Clase de riesgo	Riesgo	Descripción	Consecuencias/Efectos Potenciales
Interno - Externo	seguridad de la información 2. Falta de una adecuada capacitación para la toma de conciencia 3. Falla en los controles de seguridad informática 4. Carencia de herramientas de seguridad informática 5. Falta de plan de recuperación de desastres documentado, aprobado y materializado 6. Debilidad en la aplicación de la metodología de identificación de riesgos de seguridad de la información	Riesgo Estratégico	Falta de definición y aplicación de controles efectivos para salvaguarda de la información	El establecimiento indebido de controles efectivos de seguridad de la información y/o su inadecuada aplicación, conllevan a la pérdida de la confidencialidad, integridad y disponibilidad de la información.	1. Pérdida de la imágen institucional 2. Demandas judiciales a la Institución 3. Pérdida de recursos económicos 4. No garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información de los ciudadanos y usuarios de la Supersalud

Figura # 35 Descripción de riesgos

6.4 Clasificación de Riesgos

Algunas entidades durante el proceso de identificación del riesgo pueden hacer una clasificación de este, con el fin de establecer con mayor facilidad la

identificación de estos, además esto podría el análisis del impacto, considerado en el siguiente paso del proceso de análisis del riesgo.

Riesgo Estratégico: Se asocia con la forma en que se administra la cooperativa. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la cooperativa por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de los asociados hacia la cooperativa.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información, de la definición de los procesos, de la estructura de la cooperativa, de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la cooperativa que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la cooperativa para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad y sus asociados.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la cooperativa para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

De acuerdo con lo anterior, se recomienda que los riesgos se clasifiquen, esto con el fin de establecer si todos los riesgos han sido identificados, esto se puede identificar, si alguno de las clases riesgos no cuenta con riesgos, esto le permitirá a la cooperativa, identificar otros:

Clase de riesgo	Descripción del riesgo
Estratégico	xxx

	yyy
Imagen	
Operativo	Zzz
Financiero	Ttt
Cumplimiento	nnn
Tecnológico	ggg

En este cuadro, se puede identificar la inexistencia de riesgos de imagen, y si bien no es una regla, de que se deban identificar riesgos por cada clase, sin embargo, ayudará a preguntarse si existe alguno que no se haya identificado. Retomando los riesgos identificados en este documento, se tendría que ambos estarían dentro de los riesgos de cumplimiento.

CLASE DE RIESGO	RIESGOS
Cumplimiento	Incumplimiento en la generación de respuestas a los usuarios
Cumplimiento	Generación de respuestas inadecuadas o erróneas a los usuarios.

Una vez estructurada la información se procederá a incluir la información (Clase de Riesgo) en el formato denominado, Matriz de Riesgos de Gestión.

Tipo de factor de riesgo	Causas	Clase de riesgo	Riesgo	Descripción	Consecuencias/Efectos Potenciales
Interno - Externo	seguridad de la información 2. Falta de una adecuada capacitación para la toma de conciencia 3. Falla en los controles de seguridad informática 4. Carencia de herramientas de seguridad informática 5. Falta de plan de recuperación de desastres documentado, aprobado y materializado 6. Debilidad en la aplicación de la metodología de identificación de riesgos de seguridad de la información	Riesgo Estratégico	Falta de definición y aplicación de controles efectivos para salvaguarda de la información	El establecimiento indebido de controles efectivos de seguridad de la información y/o su inadecuada aplicación, conllevan a la pérdida de la confidencialidad, integridad y disponibilidad de la información.	1. Pérdida de la imágen institucional 2. Demandas judiciales a la Institución 3. Pérdida de recursos económicos 4. No garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información de los ciudadanos y usuarios de la Supersalud

Figura # 36 Clasificación de riesgos

6.5 Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia de este y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

El análisis del riesgo depende de la información obtenida en la fase de identificación de Riesgos, para adelantar el análisis del riesgo se deben considerar los siguientes aspectos: Calificación del riesgo y evaluación del riesgo.

6.5.1 Calificación del riesgo

Se logra mediante la estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Por *probabilidad* se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

Para la calificación del riesgo mediante la probabilidad, se deben tener en cuenta 5 niveles, los cuales se describen a continuación:

NIVEL	CONCEPTO	DESCRIPCIÓN	FRECUENCIA
1	Rara vez	Puede que no se haya presentado u ocurrir solo en circunstancias excepcionales.	Nunca o no se ha presentado en los últimos 5 años
2	Improbable	Pudo ocurrir en algún momento, es poco común o frecuente	Al menos una vez en los últimos 5 años
3	Posible	Puede ocurrir en algún momento	Al menos una vez en los últimos 2 años

4	Probable	Ocurrirá en la mayoría de las circunstancias.	Al menos una vez en el último año
5	Casi Seguro	Se espera que ocurra en la mayoría de las circunstancias	Más de una vez al año

Por *Impacto* se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Al igual que la probabilidad para el establecimiento del impacto, se presenta 5 niveles, los cuales se describen en la matriz siguiente:

	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTROFICO (5)
TIPO DE IMPACTO	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.
Imagen (Asociado con la pérdida de credibilidad)	Afecta a un grupo de funcionarios del proceso.	Afecta a todos los funcionarios de la organización.	Afecta a los usuarios de la organización.	Afecta a los usuarios del sector.	Afecta a la ciudadanía.
Seguridad de la Información (pérdida o revelación de la información)	Afecta a una persona o una actividad del proceso.	Afecta a un grupo de trabajo o algunas actividades del proceso.	Afecta el proceso.	Afecta varios procesos de la organización.	Afecta toda la organización.
Impacto legal (asociado con el cumplimiento normativo	Genera un requerimiento.	Genera investigaciones disciplinarias, y/o fiscales y/o penales.	Genera interrupciones en la prestación del bien o servicio.	Genera sanciones.	Genera cierre definitivo de la organización.
Operativo (asociados con la forma técnica y operativa de llevar a cabo las actividades)	Genera ajustes a una actividad concreta.	Genera ajustes en los procedimientos	Genera ajustes o cambios en los procesos.	Genera intermitencia en el servicio.	Genera paro total del proceso y/o de la organización.
Financiero (asociada con impactos que generen pérdidas económicas)	La pérdida financiera no afecta la operación normal de la entidad.	La pérdida financiera afecta algunos servicios administrativos	La pérdida financiera afecta parcialmente la prestación del servicio.	La pérdida financiera afecta considerablemente la prestación del servicio.	La pérdida financiera afecta totalmente la prestación del servicio.

Figura # 37 Tipo de impacto

Para tener en cuenta:

- El impacto de confidencialidad de la información se refiere a la pérdida o revelación de la misma. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la cooperativa solo puede ser conocida y difundida al interior de la misma; así mismo, la sensibilidad de la información depende de la importancia que esta tenga para el desarrollo de la misión de la cooperativa.
- El impacto de credibilidad se refiere a la pérdida de la misma frente a diferentes actores sociales o dentro de la cooperativa.
- El impacto legal se relaciona con las consecuencias legales para la cooperativa, determinadas por los riesgos relacionados con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable.
- El impacto operativo aplica en la mayoría de las organizaciones para los procesos clasificados como de apoyo, ya que sus riesgos pueden afectar el normal desarrollo de otros procesos.
- Las tablas de calificación de probabilidad e impacto se pueden modificar o ajustar según la naturaleza y características de la organización.
- La calificación inicial de probabilidad e impacto corresponde al riesgo inherente; es decir, previo a la identificación de los controles.

6.5.2 Evaluación del Riesgo

Permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la cooperativa; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Para facilitar la calificación y evaluación a los riesgos, a continuación, se presentan dos matrices que contemplan análisis cualitativo (en la primera) y cualitativo-cuantitativo (en la segunda), para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia

(probabilidad), así mismo para cada caso se presenta las opciones de manejo según la ubicación de los riesgos en las matrices.

Las categorías relacionadas con el impacto son: insignificante, menor, moderado, mayor y catastrófico. Las categorías relacionadas con la probabilidad son raro, improbable, posible, probable y casi seguro, tal y como se relacionó en las tablas anteriores.

PROBABILIDAD		IMPACTO				
		1	2	3	4	5
		Insignificante	Menor	Moderado	Mayor	Catastrófico
1	Raro	B	B	B	M	M
2	Improbable	B	M	M	A	A
3	Posible	B	M	A	A	E
4	Probable	M	A	A	E	E
5	Casi seguro	M	A	E	E	E

Figura # 38 Matriz de Calificación y evaluación de los Riesgos por zonas de riesgo

Zona de Riesgo		Opciones de manejo
B	Baja	Asumir el riesgo
M	Moderada	Reducir (medidas para llevarlo a la zona baja), asumir el riesgo
A	Alta	Evitar, reducir (medidas para llevarlo a la zona moderada), compartir o transferir el riesgo
E	Extrema	Evitar (controles preventivos que busquen reducir el nivel de probabilidad del riesgo), reducir (controles orientados a minimizar el impacto si el riesgo se materializa), compartir o transferir el riesgo (pólizas)

Figura # 39 Matriz opciones de manejo según la ubicación en las zonas de riesgo

PROBABILIDAD		IMPACTO				
		1	2	3	4	5
		Insignificante	Menor	Moderado	Mayor	Catastrófico
1	Raro	1	2	3	4	5
2	Improbable	2	4	6	8	10
3	Posible	3	6	9	12	15
4	Probable	4	8	12	16	20
5	Casi seguro	5	10	15	20	25

Figura # 40 Matriz de evaluación por zonas de riesgo (resultados probabilidad por impacto)

Los rangos se obtienen al multiplicar la probabilidad por el impacto como lo sugiere la norma ISO 31000:2009 y las zonas de riesgo son las establecidas por el DAFP, tal y como se muestra en el siguiente ejemplo:

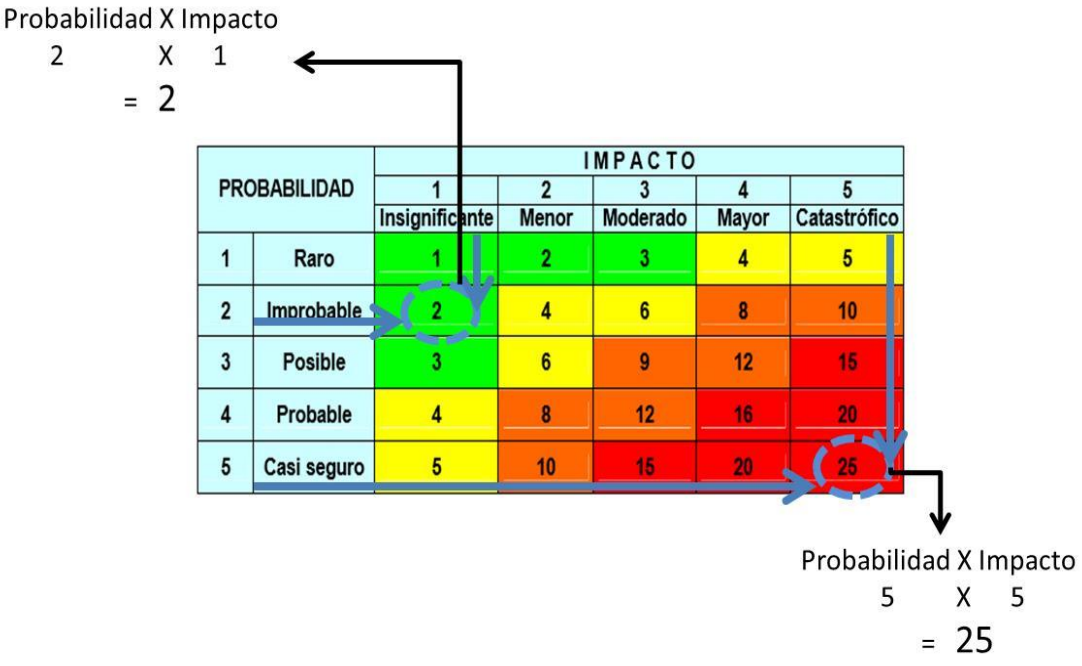


Figura # 41 Matriz de probabilidad de impacto

Como resultado de la matriz, se genera la "**Matriz de Calificación, Evaluación y Respuesta a los Riesgos"**

Rangos según resultado de la evaluación (Probabilidad por impacto)	Zona de riesgo
1 a 3	Zona de riesgo baja
4 a 6	Zona de riesgo moderada
7 a 14	Zona de riesgo alta
15 a 25	Zona de riesgo extrema

Figura # 42 Matriz de Calificación, Evaluación y Respuesta a los Riesgos

Dependiendo la ubicación numérica, se generará las Opciones de manejo según la ubicación en las zonas de riesgo.

Para el caso específico de la cooperativa FAVI, dentro del formato denominado Matriz de Riesgos de Gestión, se analiza el riesgo, en donde se califica el impacto y la probabilidad mostrando la zona de riesgo a la cual pertenece.

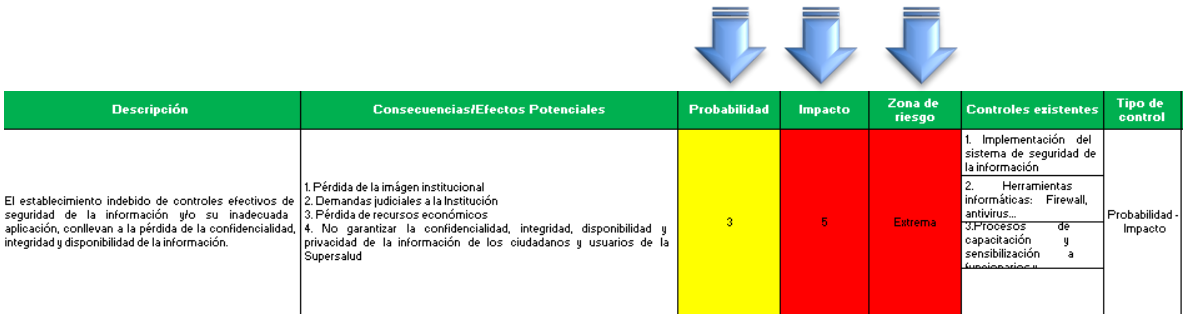
Descripción	Consecuencias/Efectos Potenciales	Probabilidad	Impacto	Zona de riesgo	Controles existentes	Tipo de control
El establecimiento indebido de controles efectivos de seguridad de la información y/o su inadecuada aplicación, conllevan a la pérdida de la confidencialidad, integridad y disponibilidad de la información.	1. Pérdida de la imágen institucional 2. Demandas judiciales a la Institución 3. Pérdida de recursos económicos 4. No garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información de los ciudadanos y usuarios de la Supersalud	3	5	Extrema	1. Implementación del sistema de seguridad de la información 2. Herramientas informáticas: Firewall, antivirus... 3.Procesos de capacitación y sensibilización a funcionarios"	Probabilidad - Impacto

Figura # 43 Probabilidad de impacto y zona de riesgo

Siguiendo con los riesgos analizados en esta guía, se puede establecer qué y tomando como referente las matrices anteriores, lo siguiente

RIESGO	PROBABILIDAD	IMPACTO
Incumplimiento en la generación de respuestas a los usuarios	Se presentó una vez en los últimos 2 años, esta situación da una probabilidad de **posible**, es decir una calificación de **3** el cual se desprende de su nivel.	El impacto es considerado como **catastrófico**, ya que afectaría a la ciudadanía en el entendido que es un riesgo de imagen, en este sentido la calificación obtenida es de 5

Con esta información, se procede a diligenciar los campos del respectivo formato denominado Matriz de Riesgos de Gestión.



Descripción	Consecuencias/Efectos Potenciales	Probabilidad	Impacto	Zona de riesgo	Controles existentes	Tipo de control
El establecimiento indebido de controles efectivos de seguridad de la información y/o su inadecuada aplicación, conllevan a la pérdida de la confidencialidad, integridad y disponibilidad de la información.	1. Pérdida de la imágen institucional 2. Demandas judiciales a la Institución 3. Pérdida de recursos económicos 4. No garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información de los ciudadanos y usuarios de la Supersalud	3	5	Extrema	1. Implementación del sistema de seguridad de la información 2. Herramientas informáticas: Firewall, antivirus... 3.Procesos de capacitación y sensibilización a funcionarios y	Probabilidad - Impacto

Figura # 44 Probabilidad de impacto y zona de riesgo

Una vez estructurada la información y de acuerdo con la metodología, se procederá a incluir en los campos (probabilidad e impacto), los resultados obtenidos. Estos campos automáticamente generarán el resultado de la zona de riesgo de acuerdo con la ponderación que se de en el análisis.

Para tener en cuenta:

- El valor de la probabilidad y el del impacto, se desprenden de las matrices correspondientes a los niveles de análisis de cada uno.
- El tipo de impacto se desprende de la columna correspondiente a este ítem de la matriz de nivel de impacto.
- La evaluación sale del cruce de probabilidad e impacto en la matriz de Calificación y evaluación de los Riesgos por zonas de riesgo
- Las Medidas de respuesta, se desprende de la matriz opciones de manejo según la ubicación en las zonas de riesgo

Para tener en cuenta

Esta calificación y evaluación inicial del riesgo es esencial y permanente

6.6 Valoración del Riesgo

Esta es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes

procesos, los cuales permiten obtener información para efectos de tomar decisiones.

Para realizar la valoración de los controles existentes, es necesario recordar que estos se clasifican en:

- **Preventivos:** aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización. (Afecta la Probabilidad)
- **Correctivos:** aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia. (Afecta el Impacto)

En la siguiente tabla se enlistan algunos controles dependiendo su tipo (fuente, Guía para la administración del riesgo DAFP)

Controles de Gestión	Políticas claras aplicadas
	Seguimiento al plan estratégico y operativo
	Indicadores de gestión
	Tableros de control
	Seguimiento al cronograma
	Evaluación del desempeño
	Informes de gestión
	Monitoreo de riesgos
Controles Operativos	Conciliaciones
	Consecutivos
	Verificación de firmas
	Listas de chequeo
	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldo
	Personal capacitado
	Aseguramiento y calidad
Controles Legales	Normas claras y aplicadas
	Control de términos

Figura # 45 Controles de administración de riesgo

Lo anterior es un referente de controles, sin embargo, en el siguiente ejemplo se presenta una forma de redacción de un control.

Causa	Riesgo	Efecto/Consecuencia	Control
Uso de un calendario tributario obsoleto.	Declaración de impuestos extemporánea	Sanciones pecuniarias para la entidad o disciplinaria para un(os) funcionario(s).	El contador y/o el subdirector administrativo y financiero debe realizar la actualización y divulgación, en enero de cada año, de los calendarios tributarios, nacionales y distritales, en página Web, Intranet, físicos, etcétera.

Figura # 46 Ejemplo de redacción de un control

Nótese que este control se centra en la causa, adicional para el análisis de controles, se utiliza el metalenguaje del riesgo, para lo cual es necesario tener en cuenta que no necesariamente deben ser concebidos controles para las causas, podrían ser concebidos para el efecto (el impacto), sin embargo, el ideal es tener un control integral, es decir donde se mitigue la causa y la consecuencia.

Los controles excesivos se generan cuando se definen múltiples acciones aisladas para atacar la causa del riesgo. Lo correcto es articular dichas acciones para que el control sea integral. Los controles deben ser:

- Objetivos: no dependen del criterio de quien lo defina y/o ejecute, sino de los resultados que se esperan obtener.
- Pertinentes: corresponden a las causas propias del riesgo.
- Económicos: costos razonables de los recursos requeridos.
- Realizables: se pueden llevar a cabo.
- Medibles: permiten el establecimiento de indicadores - Periódicos: tienen frecuencia de aplicación en el tiempo.
- Efectivos: producen impacto positivo.
- Asignables: tienen responsables.

Para el caso del ejemplo presentado en este documento, se han establecido tres controles que son:

1. Aplicativo que permite mediante alarmas, controlar las fechas límite para las respuestas a los usuarios sobre las comunicaciones escritas recibidas.
2. Plan de capacitación a los servidores, sobre la normatividad vigente y el manejo adecuado del sistema de información implementado.
3. Procedimiento formalizado de atención de respuestas a usuarios.

Adicional a ello es pertinente evaluar, si el control previene la materialización del riesgo (afecta la probabilidad) o el control permite enfrentar la situación en caso de materialización (afecta el impacto).

Una vez establecidos los controles y el tipo de control, estos deben ser evaluados de manera individual, para lo cual se deben diligenciar los documentos de trabajo anexos al formato Matriz de Riesgos de Gestión y responder tres preguntas clave:

PREGUNTAS		SI / NO	Puntaje
1.	¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	SI / NO	25% - 0%
2.	¿El control se está aplicando?	SI / NO	25% - 0%
3.	¿El control es efectivo (sirve o cumple su función)?	SI / NO	50% - 0%
TOTAL			100%

Figura # 47 Preguntas de control

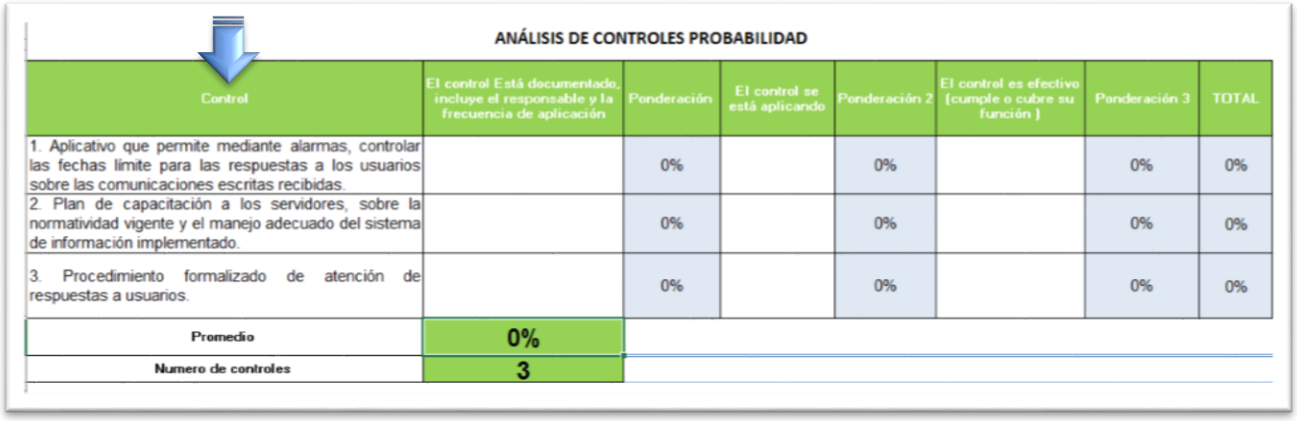
Cada una de estas preguntas, presentan únicamente dos opciones de respuestas, SI o NO, para el caso de la primera, en caso de responder SI, obtendrá un 25%, para la segunda, si responde SI, obtendrá un 25%, y para la tercera el SI, le permitirá obtener un 50%, en los tres casos la respuesta NO asignará un 0%.

En la primera pregunta cuando no se cumpla con algunos de los tres aspectos relacionados (documentado, responsable y frecuencia), se debe marcar la opción NO y el puntaje asignado será cero.

Con el fin de entender el análisis de los controles, es necesario identificar si son de causas (probabilidades) o de efectos (impacto):

Nota: Los documentos de trabajo se diligenciarán así:

1. Se determinó que los tres controles apuntan a la probabilidad.
2. En la columna control se debe diligenciar los controles, en este caso del ejemplo se transcriben los tres controles, así:

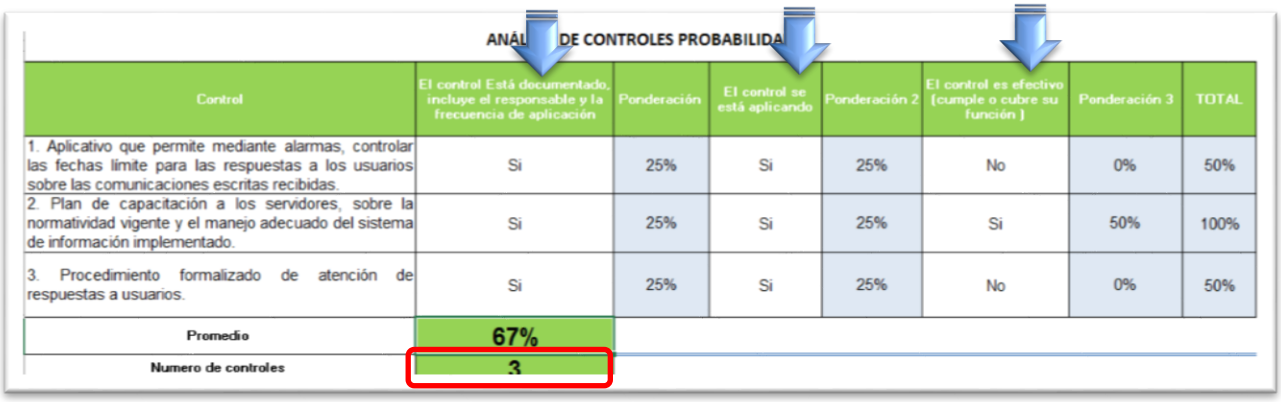


ANÁLISIS DE CONTROLES PROBABILIDAD

Control	El control Está documentado, incluye el responsable y la frecuencia de aplicación	Ponderación	El control se está aplicando	Ponderación 2	El control es efectivo (cumple o cubre su función)	Ponderación 3	TOTAL
1. Aplicativo que permite mediante alarmas, controlar las fechas límite para las respuestas a los usuarios sobre las comunicaciones escritas recibidas.		0%		0%		0%	0%
2. Plan de capacitación a los servidores, sobre la normatividad vigente y el manejo adecuado del sistema de información implementado.		0%		0%		0%	0%
3. Procedimiento formalizado de atención de respuestas a usuarios.		0%		0%		0%	0%
Promedio	0%						
Numero de controles	3						

Figura # 48 Análisis de controles de probabilidad

3. Luego de diligenciar el campo del control, procedemos a responder cada una de las preguntas, según la metodología. En este documento de trabajo se deberá seleccionar la opción si, o no, la cual se desplegaran las opciones para escogerlas.

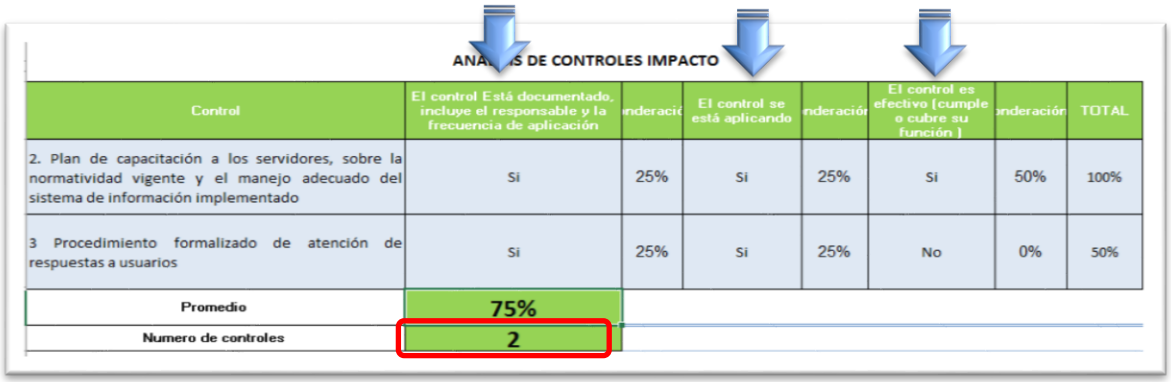


ANÁLISIS DE CONTROLES PROBABILIDAD

Control	El control Está documentado, incluye el responsable y la frecuencia de aplicación	Ponderación	El control se está aplicando	Ponderación 2	El control es efectivo (cumple o cubre su función)	Ponderación 3	TOTAL
1. Aplicativo que permite mediante alarmas, controlar las fechas límite para las respuestas a los usuarios sobre las comunicaciones escritas recibidas.	Si	25%	Si	25%	No	0%	50%
2. Plan de capacitación a los servidores, sobre la normatividad vigente y el manejo adecuado del sistema de información implementado.	Si	25%	Si	25%	Si	50%	100%
3. Procedimiento formalizado de atención de respuestas a usuarios.	Si	25%	Si	25%	No	0%	50%
Promedio	67%						
Numero de controles	3						

Figura # 49 Análisis de controles de probabilidad

4. A continuación, en las columnas Ponderación 1, Ponderación 2, Ponderación 3 y Total, se realizará automáticamente, de igual forma se calculará automáticamente el promedio, que en este ejemplo fue el “67%”, este resultado es el que se va a transcribir en la matriz de Riesgos de Gestión.
5. Igualmente se determinaron los controles para el análisis del control de impacto; en este ejemplo se tomaron los controles 2 y 3 y se siguió con la metodología. El promedio del impacto calculado fue el “75%”. este resultado es el que se va a transcribir en la matriz de Riesgos de Gestión.

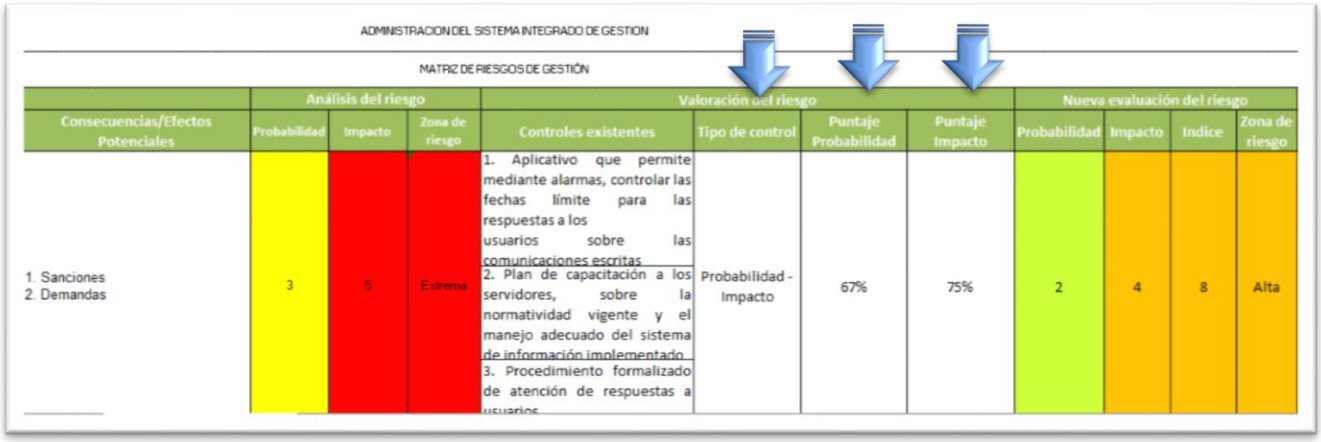


ANÁLISIS DE CONTROLES IMPACTO

Control	El control Está documentado, incluye el responsable y la frecuencia de aplicación	nderació	El control se está aplicando	nderación	El control es efectivo [cumple o cubre su función]	onderación	TOTAL
2. Plan de capacitación a los servidores, sobre la normatividad vigente y el manejo adecuado del sistema de información implementado	Si	25%	Si	25%	Si	50%	100%
3 Procedimiento formalizado de atención de respuestas a usuarios	Si	25%	Si	25%	No	0%	50%
Promedio	75%						
Numero de controles	2						

Figura # 50 Análisis de controles de impacto

6. Luego de tener estos resultados se transcriben a la matriz de Riesgos de Gestión, así:
    - Se selecciona el tipo de control, que en este caso tiene una lista desplegable (probabilidad, impacto, probabilidad – impacto)
    - Ingresa los porcentajes de impacto y probabilidad ya calculados en los documentos de trabajo. (probabilidad 67%, impacto 75%)
    - A continuación, se diligenciará automáticamente la nueva evaluación del riesgo. Sin embargo, a continuación, se describe como se realiza metodológicamente la nueva valoración del riesgo.



ADMINISTRACION DEL SISTEMA INTEGRADO DE GESTION

MATRIZ DE RIESGOS DE GESTIÓN

Consecuencias/Efectos Potenciales	Análisis del riesgo			Valoración del riesgo				Nueva evaluación del riesgo			
	Probabilidad	Impacto	Zona de riesgo	Controles existentes	Tipo de control	Puntaje Probabilidad	Puntaje Impacto	Probabilidad	Impacto	Indice	Zona de riesgo
1. Sanciones 2. Demandas	3	5	Extrema	1. Aplicativo que permite mediante alarmas, controlar las fechas límite para las respuestas a los usuarios sobre las comunicaciones escritas 2. Plan de capacitación a los servidores, sobre la normatividad vigente y el manejo adecuado del sistema de información implementado 3. Procedimiento formalizado de atención de respuestas a usuarios	Probabilidad - Impacto	67%	75%	2	4	8	Alta

Figura # 51 Análisis de controles de probabilidad

Al evaluar los controles establecidos, se generará un riesgo denominado residual, el cual se analiza una vez la probabilidad y el impacto se desplazan en la matriz de calificación y evaluación de riesgos, teniendo en cuenta el valor total desprendido de la sumatoria de los puntajes obtenidos de la aplicación de las preguntas claves, en este sentido el nivel de desplazamiento se desprende de acuerdo con los siguientes rangos de puntaje:

RANGO	Casillas que disminuyen en la Probabilidad	Casillas que disminuyen en el Impacto
0-50	0	0
51-75	1	1
76-100	2	2

Figura # 52 Rango de impacto

Para el ejemplo utilizado en esta guía, se tiene lo siguiente:

- Que la probabilidad al tener un puntaje de 67%, las casillas que disminuyen en la probabilidad es de 1.
- Que el impacto al tener un puntaje de 75%, las casillas que disminuyen en el impacto es 1

Los rangos como ya fue mencionado permiten el desplazamiento en la matriz de evaluación, de acuerdo con las siguientes características:

PROBABILIDAD		IMPACTO				
		1	2	3	4	5
		Insignificante	Menor	Moderado	Mayor	Catastrófico
1	Raro	B	B	B	M	M
2	Improbable	B	M	M	A	A
3	Posible	B	M	A	A	E
4	Probable	M	A	A	RI RR	E
5	Casi seguro	M	A	E	No hay desplazamiento	E

Figura # 53 Resultado de la evaluación en el rango 0-50

En este rango el riesgo inherente y el residual no sufre ningún desplazamiento.

PROBABILIDAD		IMPACTO				
		1	2	3	4	5
		Insignificante	Menor	Moderado	Mayor	Catastrófico
1	Raro	B	B	B	M	M
2	Improbable	B	M	M	A	A
3	Posible	B	M	A	RR	E
4	Probable	M	A	RR	RI	E
5	Casi seguro	M	A	Cuando afecta impacto	Cuando afecta probabilidad	E

Figura # 54 Resultado de la evaluación en el rango 51-75

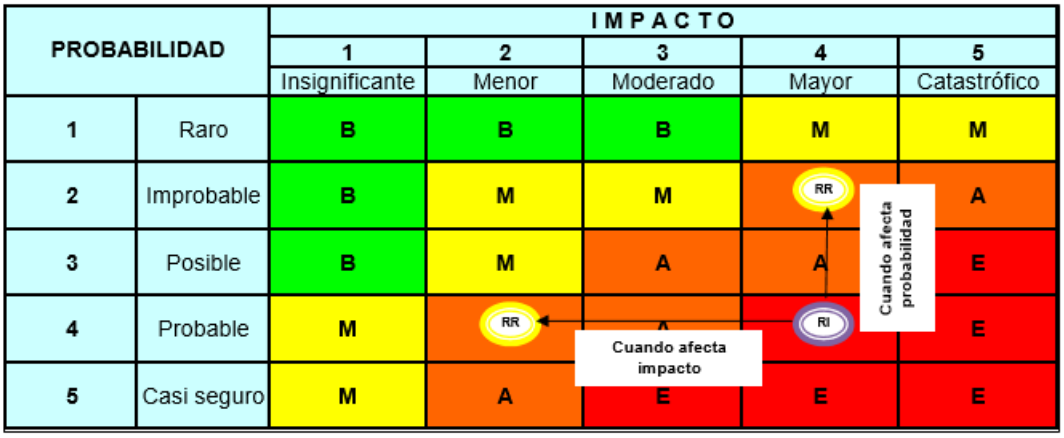


Figura # 55 Resultado de la evaluación en el rango 76-100

Para el caso del ejemplo utilizado en la presente guía la calificación inicial tanto de probabilidad y el impacto es la siguiente:

RIESGO	CALIFICACIÓN	
	Probabilidad	Impacto
Incumplimiento en la generación de respuestas a los usuarios	3	5

De acuerdo con la evaluación de los controles, se pudo establecer que la probabilidad y el impacto se moverían una casilla, por ello la nueva calificación del riesgo es la siguiente:

RIESGO	CALIFICACIÓN	
	Probabilidad	Impacto
Incumplimiento en la generación de respuestas a los usuarios	2	4

Al tener esta calificación, la nueva ubicación en la matriz de ubicación del riesgo se relaciona a continuación:

Figura # 56 Matriz de ubicación del riesgo

En la siguiente matriz, se podrá establecer el nivel desplazamiento del riesgo inherente al riesgo residual:

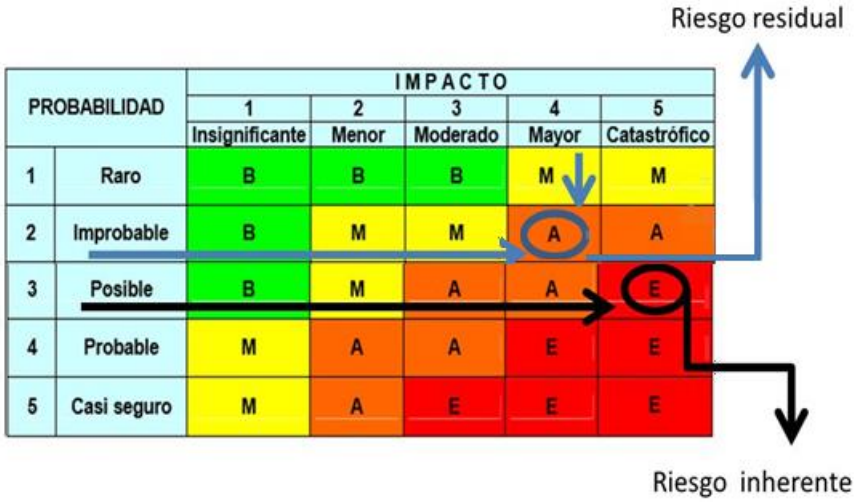


Figura # 57 Nivel de desplazamiento del riesgo inherente al riesgo residual

El resultado obtenido a través de la valoración del riesgo es denominado también tratamiento del riesgo, ya que se “involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales acciones”, así el desplazamiento dentro de la Matriz de Evaluación y Calificación determinará finalmente la selección de las opciones de tratamiento del riesgo, así:

***Evitar el riesgo**,* tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.	***Reducir el riesgo**,* implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.
***Compartir o transferir el riesgo**,* reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.	***Asumir un riesgo,*** luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Dicha selección implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales, por lo tanto, se deberá considerar los siguientes aspectos como:

- Viabilidad jurídica.
- Viabilidad técnica.
- Viabilidad institucional.
- Viabilidad financiera o económica
- Análisis de costo-beneficio.

Para el ejemplo utilizado en esta guía, se diligencia en la Matriz de Riesgos de Gestión Código A05FMR la columna tratamiento, esta columna tendrá una lista desplegable (*Evitar el riesgo*, *Reducir el riesgo,* Compartir *o transferir el riesgo,* Asumir *un riesgo),* para determinar finalmente la selección de las opciones de tratamiento del riesgo.

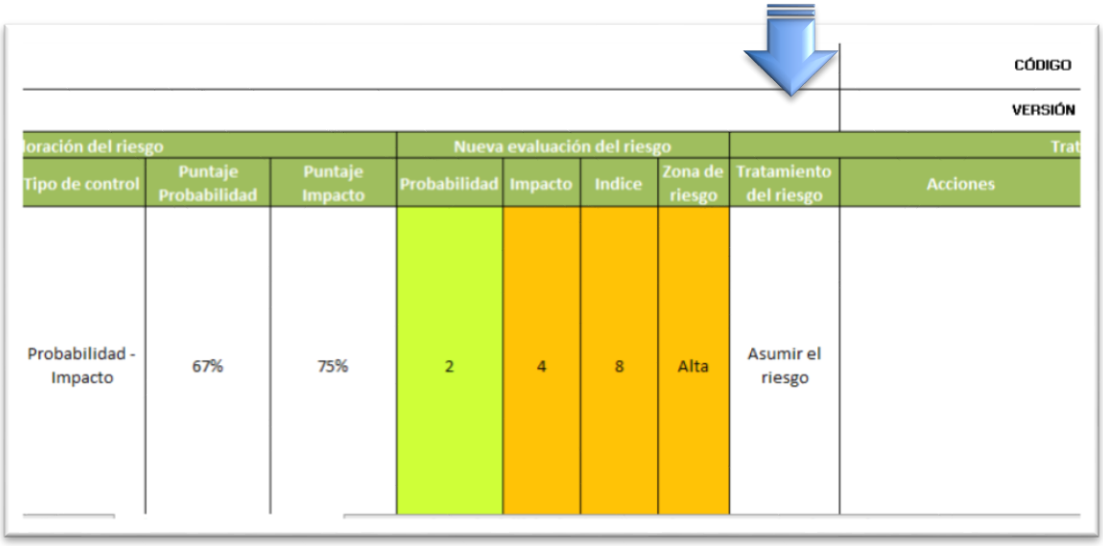


Figura # 58 Nueva evaluación del riesgo

Una vez validada las acciones del tratamiento del riesgo, se procede a definir qué acciones, frecuencia y responsable se realizarán dentro de cada control para hacer que funcione de manera adecuada, en este sentido si se toma el

control 1.1 Aplicativo que permite mediante alarmas, controlar las fechas límite para las respuestas a los usuarios sobre las comunicaciones escritas recibidas, se harán dos actividades la primera Asignación de identificaciones para uso del software por parte de los servidores del área y una segunda elaboración de cronograma de capacitación por grupos, estas actividades se harán para un período de tiempo específico de hecho el MECI:2014 recomienda efectuar una revisión anual, por lo que se podría decir que estas acciones tendrán una vigencia no superior a un año, la información aquí desprendida se incluirá posteriormente en el mapa de riesgos de gestión.

La forma de trabajar esta información se dará de la siguiente forma:

Control	Acciones
1.1 Aplicativo que permite mediante alarmas, controlar las fechas límite para las respuestas a los usuarios sobre las comunicaciones escritas recibidas	Asignación de identificaciones para uso del software por parte de los servidores del área. Elaboración de cronograma de capacitación por grupos

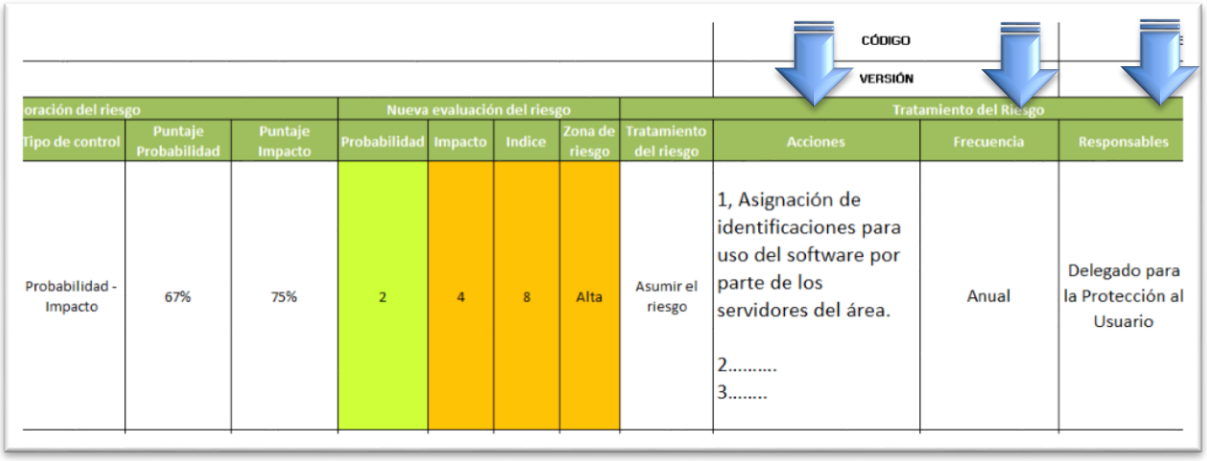


Figura # 59 Tratamiento del riesgo

7. Política de Administración de riesgos

Para la consolidación de las Políticas de Administración de Riesgos se deben tener en cuenta todas las etapas anteriormente desarrolladas.

Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de estos, permiten tomar decisiones adecuadas y fijar los lineamientos, que van a transmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la cooperativa.
Se tiene como Política de Administración del riesgo la siguiente:

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DE LA COOPERATIVA FAVI UTP

La cooperativa FAVI busca la satisfacción de sus usuarios y partes interesadas, cumpliendo los requisitos legales y organizacionales suscritos frente al Sistema de Gestión, en materia de administración de los riesgos institucionales y los de corrupción se compromete a:

1) Identificar los factores internos y externos que se puedan convertir en eventos adversos que afecten o impidan el normal desarrollo y la gestión eficaz de los procesos.
2) Valorar los riesgos, así como a la debida selección de métodos para su tratamiento y monitoreo.
3) Preservar la eficacia operativa de la cooperativa FAVI, así como la salvaguarda de sus bienes y el bienestar de sus colaboradores.
4) Garantizar el mejor manejo de los recursos, el cumplimiento de los objetivos de los procesos y el logro de los propósitos institucionales.
5) Definir estrategias de comunicación y divulgación de la administración del riesgo en la cooperativa
6) Capacitar y entrenar al talento humano de la cooperativa para una efectiva administración del riesgo.
7) Administrar los riesgos de corrupción para evitarlos o reducirlos a través de acciones encaminadas a prevenir su materialización o disminuir la probabilidad e impacto de materialización.

Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

DECLARACIÓN DE APLICABILIDAD

La presente declara los controles que son relevantes para el SGSI de la cooperativa y aplicables al mismo.

Adicionalmente en ella se encuentran justificada la aplicación o la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades empresariales de la organización en materia de seguridad de la información:

L: Requerimiento Regulatorio

C: Obligación contractual

N: Requerimiento del negocio

R: Análisis de riesgos

ISO #	Sección	Control	#	Aplicabilidad	Justificación	L	C	N	R
A.5	**Políticas de Seguridad**								
A.5.1	**Orientación de la Dirección para la Gestión de la Seguridad de la Información**								
A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	1	SI	Se redactan los documentos: "Políticas del SGSI y Políticas de tercer nivel de seguridad de la información" con el fin de socializar a los funcionarios de la cooperativa el compromiso que deben tener respecto a la seguridad de la información y los riesgos a los que se está expuesta.	x		x	

A.5.1.2	Revisión de las políticas de seguridad de la información	Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	2	SI	Una vez socializada la política de seguridad de la información se debe implementar un procedimiento de revisión en unos intervalos de tiempo con el fin de asegurar que se cumpla efectivamente.	x		x	
A.6	**Organización de la seguridad de la información**								
A.6.1	**Organización interna**								
A.6.1.1	Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	3	SI	Por medio del documento: "Matriz de roles y responsabilidades" se establecen los compromisos de los diferentes funcionarios respecto al sistema de seguridad de la información asignando responsabilidades para el cumplimiento de la misma			x	
A.6.1.2	Separación de deberes	Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	4	SI	De igual forma se debe mantener protegida la información por medio de la revisión del SGSI y pactar acuerdos de confidencialidad por parte de los funcionarios.			x	
A.6.1.3	El contacto con las autoridades	Se debe mantener contactos apropiados con las autoridades pertinentes.	5	SI	Como principio de seguridad de la información, cumplir con la regulación del Gobierno colombiano, además de contar con entidades externas que prestan servicios de TI, se debe contar con este control implementado.	x			

A.6.1.4	El contacto con los grupos de interés especial	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	6	SI	Se establece el documento: "Contacto con las autoridades y grupos de interés especial" con el fin de controlar incidentes de seguridad de la información a mayor escala.			x	
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto.	7	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad, se debe contar con este control implementado.				x
A.6.2	**Los dispositivos móviles y el teletrabajo**								
A.6.2.1	Política de dispositivo móvil	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	8	SI	En el documento: "Políticas de tercer nivel de seguridad de la información" se establecen las restricciones de conexión y de dispositivos móviles de funcionarios de la cooperativa.				x
A.6.2.2	El teletrabajo	Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	9	NO			x		
A.7	**La seguridad de los recursos humanos**								
A.7.1	**Antes de empleo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.**								

A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	10	SI	En el proceso de contratación se establecen acuerdos de confidencialidad que deben ser firmados por los nuevos funcionarios, a su vez se establece el formato de paz y salvo en el cual una vez finalizado su contrato se establece un control sobre los activos de información a la que este tiene acceso.		x		
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	11	SI			x		
A.7.2	**Durante la ejecución del empleo**								
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	12	SI	Los funcionarios y proveedores de la cooperativa deben ser conscientes de los riesgos, responsabilidades y deberes respecto a la seguridad de la información. Se hace necesario capacitar al personal respecto a las políticas y el sistema de gestión de seguridad de la información en general y establecer un proceso			x	

A.7.2.2	Toma de conciencia, educación y formación de la Seguridad de la Información.	Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	13	SI	disciplinario respecto al actuar frente alguna violación de seguridad.			x	
A.7.2.3	proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	14	SI			x		
A.7.3	**Terminación y cambio de empleo**								
A.7.3.1	Responsabilidades en la terminación o cambio del empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	15	SI	Se establece el formato de paz y salvo en el cual los funcionarios una vez finalizado su contrato o en caso de renuncia esta entrega los activos de información los cuales le fueron entregados y en el cual informa a su supervisor para proceder a bloquear el acceso y retirar la estación de trabajo para la realización de copias de seguridad.		x		
A.8	**Gestión de activos**								
A.8.1	**La responsabilidad por los activos**								

A.8.1.1	Inventario de los bienes	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	16	SI	Se identifica plenamente los propietarios de los activos de información, se cuenta con un inventario, pero este debe ser documentado de manera detallada estableciendo reglas para su buen uso y considerando las reglas documentadas en la matriz de riesgos.				x
A.8.1.2	Propiedad de los bienes	Los activos mantenidos en el inventario deben tener un propietario.	17	SI					x
A.8.1.3	El uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	18	SI					x
A.8.1.4	Categorías de los activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	19	SI	Finalizado el contrato o relación con la cooperativa, el propietario entrega su estación de trabajo para la adecuación al respectivo uso que se le dé.				x
A.8.2	**Clasificación de la información**								
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	20	SI	La información se debe clasificar de acuerdo con su nivel de importancia y a su vez se debe implementar controles adecuados para su protección.				x

A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	21	SI					x
A.8.2.3	Manipulación de los activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	22	SI					x
A.8.3	**La gestión de medios**								
A.8.3.1	Gestión de soportes extraíbles	Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	23	SI	De acuerdo con la operación y actividades realizadas por los funcionarios, el almacenamiento e intercambio de información es efectuado a través de correo electrónico, servicios de mensajería, unidades extraíbles, entre otros. Se debe entonces promover el manejo apropiado de estos medios para evitar posibles incidentes como divulgación, perdida o modificación de información propia de la cooperativa.				x
A.8.3.2	Disposición de los medios de comunicación	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	24	SI					x
A.8.3.3	transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	25	SI					x
A.9	**Control de acceso**								
A.9.1	**Los requisitos de negocio para el control de acceso**								

A.9.1.1	política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	26	SI	Se tienen políticas establecidas de acceso a instalaciones físicas, sistemas de información y servicios en red, tales como claves de acceso, validación de entrada y salida de usuarios y datos, conexión medida, cierre de sesiones, entre otros.	x		x	
A.9.1.2	El acceso a las redes y servicios de red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	27	SI					x
A.9.2	**gestión de acceso de los usuarios**								
A.9.2.1	El registro de usuario y la cancelación de la matrícula	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	28	SI	Existen documentadas guías de acceso a redes y servicios en red y guía de gestión segura de usuarios en las cuales se establece la gestión de acceso a usuarios a cargo de la coordinación de sistemas, así como lineamientos para la asignación de perfiles, privilegios y alta y baja de usuarios.				x
A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	29	SI					x
A.9.2.3	Gestión de derechos de acceso privilegiados	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	30	SI					x
A.9.2.4	Gestión de la información de autenticación de secreto de los usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	31	SI					x

A.9.2.5	Revisión de los derechos de acceso de los usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	32	SI					x
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	33	SI					x
A.9.3	**responsabilidades de los usuarios**								
A.9.3.1	El uso de información secreta para la autenticación	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	34	SI	Se establecen periódicamente controles de acceso por parte de los funcionarios para controlar casos como retiro, perdida, modificación o divulgación de claves.				x
A.9.4	**Control de acceso a los sistemas y aplicaciones**								
A.9.4.1	restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	35	SI	Se definen políticas para controlar el acceso a la información, así como se establecen los responsables de la misma para establecer los privilegios sobre la información.				x
A.9.4.2	Procedimiento de ingreso (log-on) seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	36	SI				x	x
A.9.4.3	sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la	37	SI				x	x

		calidad de las contraseñas.							
A.9.4.4	El uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	38	SI				x	
A.9.4.5	Control de acceso al código fuente del programa	Se debe restringir el acceso a los códigos fuente de los programas.	39	SI				x	x
A.10	**Criptografía**								
A.10.1	**controles criptográficos**								
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	40	NO	No se cuenta con gestión de claves o controles criptográficos para la protección de información de la cooperativa.				x
A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	41	NO					x
A.11	**La seguridad física y ambiental**								
A.11.1	**Las áreas seguras**								
A.11.1.1	perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	42	SI	Se tienen establecidos controles de seguridad en las dos sedes de la cooperativa, se tiene monitoreo de cámaras de seguridad y el acceso está controlado por medio de clave de autenticación			x	

A.11.1.2	controles de entrada físicos	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	43	SI	controlado por empresa de seguridad externa que vigila el acceso.			x	
A.11.1.3	Asegurar oficinas, salas e instalaciones	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	44	SI				x	
A.11.1.4	La protección contra amenazas externas y ambientales	Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	45	SI				x	
A.11.1.5	El trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	46	SI				x	
A.11.1.6	Zonas de entrega y carga	Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	47	NO	No se cuenta con este tipo de áreas			x	
A.11.2	**Equipo**								
A.11.2.1	emplazamiento y la protección del equipo	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	48	SI	Se establece una guía de seguridad física y del entorno, así como un formato de ingreso a áreas seguras de tecnología en las cuales se describe forma en que los funcionarios, contratistas y visitantes deben ingresar a las instalaciones de la cooperativa FAVI UTP y asegurar solamente el ingreso de personal o			x	x

A.11.2.2	Apoyo a los servicios públicos	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	49	SI	visitantes autorizados a las diferentes dependencias al igual que en las áreas catalogadas como seguras.			x	
A.11.2.3	la seguridad de cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	50	SI				x	x
A.11.2.4	Mantenimiento de equipo	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	51	SI				x	x
A.11.2.5	La eliminación de los activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa	52	SI				x	x
A.11.2.6	La seguridad de los equipos y activos fuera del establecimiento	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	53	SI		x	x	x	x
A.11.2.7	La eliminación segura o la reutilización de los equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	54	SI	En las políticas de tercer nivel del SGSI se establecen estas directrices.				x

A.11.2.8	equipos de usuario desatendida	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	55	SI				x	x
A.11.2.9	Claro escritorio y la política de pantalla transparente	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	56	SI				x	
A.12	**seguridad de las operaciones**								
A.12.1	**los procedimientos y las responsabilidades operativas**								
A.12.1.1	procedimientos operativos documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	57	SI	Se deben establecer controles para no comprometer la seguridad ni la operación de los funcionarios. De acuerdo con las necesidades se establece un control sobre posibles eventos, se hace seguimiento y se realizan los ajustes correspondientes.			x	x
A.12.1.2	Gestión del cambio	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	58	SI		x		x	x
A.12.1.3	Gestión de la capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	59	SI		x		x	
A.12.1.4	La separación de desarrollo prueba y entornos operativos	Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	60	SI		x		x	x
A.12.2	**Protección contra el malware**								

A.12.2.1	Los controles contra el malware	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	61	SI	Los equipos cuentan con protección de software de detección y reparación de virus el cual está en constante funcionamiento para garantizar la seguridad.			x	
A.12.3	**Apoyo**								
A.12.3.1	copia de seguridad de información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	62	SI	Se cuenta con procedimientos de back ups y recuperación que permite recuperar y restaurar la información ante un posible incidente y por sobre todo garantizar la continua operación.	x	x	x	x
A.12.4	**Registro y supervisión**								
A.12.4.1	El registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	63	SI	Se deben establecer directrices respecto al análisis, evaluación y gestión del riesgo.			x	x
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	64	SI				x	x
A.12.4.3	Administrador y operador registros	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	65	SI				x	x

A.12.4.4	sincronización de los relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	66	SI				x	x
A.12.5	**El control de software operacional**								
A.12.5.1	La instalación de software en los sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	67	SI	Se debe establecer un procedimiento documentado de instalación de software, este se realiza de forma informal por parte del ingeniero de sistemas de la cooperativa.			x	x
A.12.6	**La gestión técnica de la vulnerabilidad**								
A.12.6.1	Gestión de vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	68	SI	Se establece la matriz de riesgos con controles de acción para dar respuesta a una vulnerabilidad.				x
A.12.6.2	Restricciones sobre la instalación de software	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	69	SI	Solo se permite la instalación de software licenciado.				x
A.12.7	**consideraciones de auditoría de sistemas de información**								
A.12.7.1	sistemas de información de los controles de auditoría	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las	70	NO	No se tiene previsto una auditoria por un ente externo, se realizarán periódicamente evaluaciones por parte de sistemas y control interno una vez se termine la fase de diseño y se implemente el SGSI.				x

		interrupciones en los procesos del negocio.							
A.13	**seguridad de las comunicaciones**								
A.13.1	**gestión de seguridad de la red**								
A.13.1.1	controles de red	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	71	SI	Se tienen controles de seguridad en los servicios de red con el fin de garantizar la integridad, disponibilidad e integridad de la información en la cooperativa.			x	x
A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	72	SI				x	x
A.13.1.3	La segregación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	73	SI				x	x
A.13.2	**La transferencia de información**								
A.13.2.1	políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	74	SI	Tanto en los contratos de funcionarios, como en los contratos con proveedores se establecen acuerdos donde se da un control que garantice la integridad, disponibilidad y confidencialidad de la información.				x

A.13.2.2	Los acuerdos sobre la transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	75	SI					x
A.13.2.3	La mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	76	SI	Dentro de las políticas del SGSI se establecen controles para proteger la información propia de la cooperativa, se debe socializar con los funcionarios las buenas prácticas de preservación de la información.				x
A.13.2.4	Los acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	77	SI					x
A.14	**Sistema de adquisición, desarrollo y mantenimiento**								
A.14.1	**Los requisitos de seguridad de los sistemas de información**								
A.14.1.1	Información de análisis de requisitos de seguridad y las especificaciones	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	78	SI	Si el desarrollo de aplicativos es a mayor escala o en caso de requerirse mejora en la tecnología presente, la cooperativa terceriza a un proveedor externo su consecución, estableciendo previamente controles de seguridad al aprobar los requisitos del negocio antes de implementar dichos cambios en la			x	x

A.14.1.2	Asegurar servicios de aplicaciones en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	79	SI	tecnología y exigiendo a dichos proveedores la seguridad respectiva de dicha tecnología.				x
A.14.1.3	La protección de las transacciones de servicios de aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	80	SI					
A.14.2	**Seguridad en los procesos de desarrollo y soporte**								
A.14.2.1	la política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	81	SI	El área de sistemas de la cooperativa terceriza el desarrollo de software a mayor escala estableciendo y exigiendo los lineamientos de buenas prácticas de desarrollo y construcción de sistemas de información seguros			x	x

A.14.2.2	los procedimientos de control de cambios de sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	82	SI	Si el desarrollo es de menor escala, se realiza un análisis previo que permita ejercer controles de seguridad ante los riesgos previstos con el fin de garantizar la seguridad, una vez se lleve a cabo un desarrollo este debe tener versonamientos aprobados por el coordinador de sistemas con el fin de controlar los cambios y realizar pruebas a fin de no comprometer la seguridad, modificación, perdida o divulgación de información.				x
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	83	SI				x	x
A.14.2.4	Las restricciones a los cambios en los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	84	SI				x	
A.14.2.5	principios de ingeniería de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	85	SI				x	

A.14.2.6	entorno de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	86	NO	La cooperativa por lo general terceriza el desarrollo de software por lo que no se considera necesario un control para la protección de la información.				x
A.14.2.7	desarrollo externalizado	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	87	SI	A fin de tercerizar parte de los riesgos presentes y proteger el acceso al codigo fuente de los aplicativos o sistemas, para evitar su alteración o uso mal intencionado.			x	
A.14.2.8	las pruebas de seguridad del sistema	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	88	SI	Se establecen controles de pruebas con el fin de garantizar la integridad de la información presente en los sistemas de información.				x
A.14.2.9	Sistema de pruebas de aceptación	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	89	SI	Se realizan pruebas antes de poner en operación los sistemas de información, en caso de ser una mejora o actualización tecnológica o de un sistema de información, la cooperativa trabaja en paralelo tanto con la mejora como con el sistema presente a fin de garantizar la seguridad, disponibilidad e integridad.				x
A.14.3	**Datos de prueba**								

A.14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	90	SI	Se realizan pruebas con datos modificados antes de salir a operación, una vez hechas las pruebas y verificando que el sistema funcione correctamente, estos datos modificados son eliminados y se procede a migrar la información real.				x
A.15	relaciones con los proveedores								
A.15.1	**seguridad de la información en relación con los proveedores**								
A.15.1.1	la política de seguridad de la información de relaciones con los proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	91	SI	La cooperativa exige a sus proveedores el cumplimiento de buenas prácticas y establece acuerdos y políticas en el contrato garantizando que en los requisitos del negocio está presente la seguridad de la información e infraestructura en la cual esta soportada.			x	
A.15.1.2	Dirigiéndose a la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	92	SI				x	
A.15.1.3	cadena de la tecnología de información y comunicación de suministro	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	93	SI				x	
A.15.2	**la gestión de la prestación de servicios de proveedores**								

A.15.2.1	El seguimiento y la revisión de los servicios de proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	94	SI				x	
A.15.2.2	La gestión de cambios en los servicios de proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	95	SI				x	
A.16	**gestión de incidentes de seguridad de información**								
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**								
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	96	SI	Se responde a los incidentes de seguridad de manera informal, para lo cual se establecen las políticas de seguridad que garanticen una respuesta óptima.			x	
A.16.1.2	Informar sobre los eventos de seguridad de información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	97	SI	Se debe implementar un procedimiento de análisis, evaluación y gestión de riesgos periódicamente.				x

A.16.1.3	Informes debilidades de seguridad de información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	98	SI						x
A.16.1.4	La evaluación y la decisión sobre los eventos de seguridad de información	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	99	SI						x
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	100	SI						x
A.16.1.6	Aprender de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	101	SI						x
A.16.1.7	El acopio de pruebas	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	102	SI						x
A.17	**los aspectos de seguridad de información de gestión de la continuidad del negocio**									
A.17.1	**la continuidad seguridad de la información**									

A.17.1.1	Los datos de proyección de continuidad de seguridad	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	103	SI	La cooperativa cuenta con controles de continuidad de su operación a fin de evitar cualquier tipo de interrupción en sus actividades por fallas tecnológicas importantes o desastres y con el propósito de disminuir el impacto generado.			x	
A.17.1.2	La aplicación de la información de seguridad de continuidad	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	104	SI				x	
A.17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	105	SI				x	
A.17.2	**redundancias**								
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	106	SI	Se cuenta con controles que garantizan la disponibilidad de los sistemas de información.			x	x
A.18	**Conformidad**								
A.18.1	**El cumplimiento de los requisitos legales y contractuales**								

A.18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	107	SI				x	
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	108	SI				x	
A.18.1.3	Protección de los registros	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	109	SI				x	
A.18.1.4	Privacidad y protección de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige y la legislación y la reglamentación pertinentes, cuando sea aplicable.	110	SI				x	

A.18.1.5	Reglamento de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	111	NO	La administración de claves no se realiza mediante uso de controles criptográficos.				x
A.18.2	**opiniones seguridad de la información**								
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	112	SI	Se establecen controles de mejora en el diseño del SGSI, una vez implementado se procederá a garantizar su cumplimiento.	x		x	
A.18.2.2	El cumplimiento de las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	113	SI		x		x	
A.18.2.3	revisión de cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	114	SI		x		x	

CONCLUSIONES

Es de notar, que una buena implementación de un Sistema de Gestión de Seguridad de la Información brinda a las organizaciones la habilidad de reducir los riesgos y crisis, gracias a las herramientas que permiten detectar tempranamente sus causas.

El diagnóstico realizado por medio de la lista de chequeo permite evidenciar el nivel de cumplimiento por parte de la Cooperativa hacia los requerimientos establecidos por la norma, lo que lo convierte en una medida que debe efectuarse en diferentes periodos de tiempos a fin de tener una evaluación que ayude a tomar medidas respectivas.

La cooperativa actualmente se encuentra en fase de diseño del SGSI por lo cual se hace necesario designar cada vigencia los recursos necesarios para el adecuado funcionamiento del Sistema de Seguridad de la Información una vez este sea implementado.

Se debe recalcar que no es posible la implementación de un SGSI, ni establecer un tratamiento de riesgos y aplicar controles si por parte de la alta dirección y funcionarios no se le da la debida importancia a la seguridad de la información por lo que cada vigencia la coordinación de Sistemas deberá plantear un programa anual de capacitaciones en seguridad, el cual contempla entre otras, capacitaciones especificas en temas de seguridad de la información a toda la cooperativa y campañas de sensibilización; de igual manera se debe fomentar la participación en las charlas de inducción a los nuevos funcionarios de la cooperativa, en la cual se sensibiliza a los funcionarios acerca de los lineamientos que da el Sistema de Seguridad de la Información, esto a fin de que se cumplan las políticas y procedimientos establecidas para el cumplimiento por parte de los funcionarios de la cooperativa.

De igual manera el Sistema de Seguridad está en constante mejora conforme a los factores tanto internos como externos que afectan al sistema. El Sistema de Seguridad de la Información, debe recopilar toda la información de cumplimiento de la norma a fin de mitigar los riesgos y cumplir con los objetivos organizacionales.

BIBLIOGRAFIA

[1] Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC - Modelo de Seguridad y Privacidad de la Información (MSPI). Disponible en web http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

[2] ICONTEC, Manual Directrices de Gestión del riesgo, complementa la NTC 5254:2006. 2007.

[3] NTC-ISO/IEC 27000:2014, Tecnología de la Información. Técnicas de Seguridad Sistemas de gestión de seguridad de información. Descripción y vocabulario.

[4] ICONTEC, NTC-ISO/IEC 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

[5] NTC-ISO/IEC 27005:2011, Tecnología de la Información. Técnicas de Seguridad. Administración de Riesgos de Seguridad de la Información.

[6] ICONTEC, NTC-ISO/IEC 31000. La gestión de riesgos, principios y directrices.

[7] ICONTEC, NTC-ISO/IEC Guía 73:2009 Gestión del Riesgo. Vocabulario.

[8] ICONTEC, NTC 5254 Gestión del Riesgo.

[9] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Manual de Implementación del Modelo Estándar de Control Interno para el Estado Colombiano, MECI: 2014, Mayor 2014, página web www.dafp.gov.co.

[10] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP). Disponible en web www.dafp.gov.co.

[11] DEPARTAMENTO NACIONAL DE PLANEACIÓN, Política Nacional de Seguridad Digital – CONPES 3854. Disponible en web www.dnp.gov.co

[12] Supersalud. Subsistema de Seguridad en la Información. Disponible en web https://www.supersalud.gov.co/es-co/superintendencia/sistema-integrado-de-gestion/subsistema-de-seguridad-en-la-informacion

[13] Guía de Administración del Riesgo, VEEDURÍA DISTRITAL, 2013.

[14] AS/NZS 4360:1999 Estándar Australiano Administración de Riesgos.

[15] Universidad Tecnológica de Pereira. “Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda”. Disponible en web http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf

[16] Escuela Colombiana de Ingeniería Julio Garavito. “Diseño de un sistema integrado de gestión basado en las normas ISO 9001:2015 e ISO 27001:2013 para la empresa La Casa del Ingeniero LCI”. Disponible en web https://repositorio.escuelaing.edu.co/bitstream/001/393/1/EC-%20Especilizaci%C3%B3n%20en%20Gesti%C3%B3n%20Integrada%20QHSE%20-1070954687.pdf

[17] Advisera. “27001 Academy”. Disponible en web https://advisera.com/27001academy/es/

[18] Blog especializado en Sistemas de Gestión de Seguridad de la Información. Disponible en web http://www.pmg-ssi.com/2015/07/que-es-sgsi/

[19] Cooperativa FAVI UTP. Disponible en web http://faviutp.com/quienes-somos/

[20] Bureau veritas. ISO 9001. Disponible en web http://www.bureauveritas.es/home/about-us/our-business/our-business-certification/area-of-activity/quality/calidad-iso+9001

[21] Universidad Cooperativa de Colombia. Sistema de Gestión de Calidad. Disponible en web http://www.ucc.edu.co/sistema-gestion-integral/Paginas/sistema-gestion-calidad.aspx

[22] Wikipedia. Sistema de gestión de seguridad de la información. Disponible en web https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

[23] Colombia Compra. Alcance SGSI. Disponible en web. https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documentos/20160623alcancedelsgsi.pdf